ESET MAIL SECURITY

POUR MICROSOFT EXCHANGE SERVER

Manuel d'installation et guide de l'utilisateur

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Cliquez ici pour télécharger la dernière version de ce document.



ESET MAIL SECURITY

Service client : www.eset.com/support

RÉV. 21/10/2015

Table des

Table des

1. Introduction

ESET Mail Security 6 pour Microsoft Exchange Server est une solution intégrée qui protège les boîtes aux lettres de différents types de contenu malveillant, y compris les pièces jointes infectées par des vers ou des chevaux de Troie, les documents contenant des scripts malveillants, le hameçonnage et le courrier indésirable. ESET Mail Security fournit trois types de protection : antivirus, antispam et règles définies par l'utilisateur. ESET Mail Security filtre le contenu malveillant au niveau du serveur de messagerie, avant qu'il arrive dans la boîte de réception du destinataire, sur le client.

ESET Mail Security prend en charge Microsoft Exchange Server versions 2003 et ultérieures, ainsi que Microsoft Exchange Server dans un environnement en cluster. Dans les versions récentes (Microsoft Exchange Server 2003 et versions ultérieures), les rôles spécifiques (mailbox, hub, edge) sont également pris en charge. Vous pouvez gérer ESET Mail Security à distance dans des réseaux de grande taille grâce à ESET Remote Administrator.

ESET Mail Security fournit non seulement la protection de Microsoft Exchange Server, mais également tous les outils nécessaires à la protection du serveur proprement dit (protection résidente, protection de l'accès à Internet et protection du client de messagerie).

1.1 Nouveautés de la version 6

- Gestionnaire de quarantaine de messages : l'administrateur peut inspecter les objets situés dans cette section de stockage et choisir de les supprimer ou de les libérer. Cette fonctionnalité simplifie la gestion des messages électroniques mis en quarantaine par l'agent de transport.
- Interface Web Quarantaine de messages : version Web pouvant être utilisée à la place du gestionnaire de quarantaine de messages.
- Moteur antispam : ce composant essentiel a été repensé et est désormais développé en interne.
- Analyse de base de données à la demande : l'analyseur de base de données à la demande utilise l'API des services Web Exchange pour se connecter à Microsoft Exchange Server via les protocoles HTTP/HTTPS.
- Règles **:** cette option de menu permet aux administrateurs de définir manuellement les conditions de filtrage des messages électroniques et les actions à exécuter sur les messages électroniques filtrés. Les règles de la dernière version d'ESET Mail Security ont été entièrement reconçues avec une approche différente.
- ESET Cluster : à l'instar d'ESET File Security 6 pour Microsoft Windows Server, l'ajout de stations de travail à des nœuds permet une automatisation supplémentaire de la gestion en raison de la distribution possible d'une stratégie de configuration à tous les membres du cluster. La création de clusters est possible à l'aide du nœud installé. Les clusters peuvent ensuite installer et initier tous les nœuds à distance. Les produits serveur d'ESET peuvent communiquer les uns avec les autres et échanger des données (configuration et notifications, par exemple), ainsi que synchroniser les données nécessaires pour le fonctionnement correct d'un groupe d'instances de produit. Une même configuration du produit peut donc être utilisée pour tous les membres d'un cluster. ESET Mail Security prend en charge les clusters de basculement Windows ou d'équilibrage de la charge réseau. Vous pouvez également ajouter manuellement des membres ESET Cluster sans Cluster Windows spécifique. Les clusters ESET Cluster fonctionnent dans les environnements de domaine et de groupe de travail.
- Analyse du stockage : analyse tous les dossiers partagés sur le serveur local. Vous pouvez sélectionner facilement pour l'analyse uniquement les données utilisateur stockées sur le serveur de fichiers.
- Installation basée sur les composants : vous pouvez sélectionner les composants à ajouter ou supprimer.
- Exclusions des processus - exclut des processus spécifiques de l'analyse antivirus à l'accès. En raison du rôle essentiel que jouent les serveurs dédiés (serveur d'applications, serveur de stockage, etc.), des sauvegardes régulières sont obligatoires pour garantir une reprise après incident dans les meilleurs délais. Pour accélérer les sauvegardes et garantir l'intégrité du processus et la disponibilité du service, certaines techniques, qui entrent en conflit avec la protection antivirus au niveau des fichiers, sont utilisées pendant les sauvegardes. Des problèmes identiques peuvent se produire lors des migrations dynamiques de machines virtuelles. La seule solution efficace pour éviter ces situations consiste à désactiver le logiciel antivirus. En excluant des processus spécifiques (ceux

de la solution de sauvegarde, par exemple), toutes les opérations sur les fichiers de ces processus exclus sont ainsi ignorées et considérées comme étant sûres, ce qui limite l'interférence avec le processus de sauvegarde. Il est recommandé de faire preuve de prudence lors de la création des exclusions. En effet, un outil de sauvegarde qui a été exclus peut accéder à des fichiers infectés sans déclencher d'alerte. C'est d'ailleurs la raison pour laquelle des autorisations étendues ne sont permises que dans le module de protection en temps réel.

- ESET Log Collector : collecte automatiquement les informations telles que la configuration et les nombreux journaux d'ESET Mail Security. En facilitant la collecte des informations de diagnostic, ESET Log Collector simplifie le travail de résolution des problèmes pour les techniciens ESET.
- eShell (ESET Shell) : eShell 2.0 est désormais disponible dans ESET Mail Security. eShell est une interface à ligne de commande qui offre aux utilisateurs expérimentés et aux administrateurs des options plus complètes pour gérer les produits serveur ESET.
- Analyse Hyper-V : il s'agit d'une nouvelle technologie qui permet d'analyser les disques d'une machine virtuelle sur Microsoft Hyper-V Server sans nécessiter le moindre agent sur cette machine virtuelle spécifique.

1.2 Pages d'aide

Cher utilisateur, bienvenue dans ESET Mail Security. Ce guide a pour objectif de vous aider à optimiser l'utilisation de ESET Mail Security.

Les rubriques de ce guide sont divisées en plusieurs chapitres et sous-chapitres. Vous trouverez des informations pertinentes en parcourant le **Sommaire** des pages d'aide. Vous pouvez également utiliser l'**Index** pour naviguer à l'aide des mots-clés ou utiliser la **Recherche** en texte intégral.

Pour obtenir des informations sur une fenêtre du programme dans laquelle vous vous trouvez, appuyez simplement sur la touche F1 du clavier. La page d'aide relative à la fenêtre actuellement affichée apparaîtra.

ESET Mail Security permet de rechercher une rubrique dans les pages d'aide au moyen de mots-clés ou en tapant des mots ou des expressions depuis le guide de l'utilisateur. La différence entre ces deux méthodes est qu'un mot-clé peut être associé à des pages d'aide qui ne contiennent pas le mot-clé précis dans le texte. La recherche de mots et expressions examine le contenu de toutes les pages et affiche uniquement les pages contenant effectivement le mot ou l'expression en question.

1.3 Méthodes utilisées

Les trois méthodes suivantes sont utilisées pour analyser les messages électroniques :

- Protection de la base de données de boîtes aux lettres : anciennement appelée analyse de boîtes aux lettres via VSAPI. Ce type de protection est uniquement disponible pour Microsoft Exchange Server 2010, 2007 et 2003 avec le rôle serveur de boîte aux lettres (Microsoft Exchange 2010 et 2007) ou serveur principal (Microsoft Exchange 2003). Ce type d'analyse peut être effectué sur une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend le rôle de serveur de boîte aux lettres ou de serveur principal).
- Protection du transport des messages : anciennement appelée filtrage de messages au niveau du serveur SMTP. Cette protection est assurée par l'agent de transport et est uniquement disponible pour Microsoft Exchange Server 2007 ou version ultérieure avec le rôle serveur de transport Edge ou serveur de transport Hub. Ce type d'analyse peut être effectué sur une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend un des rôles de serveur indiqués).
- Analyse de base de données à la demande : permet d'exécuter ou de planifier une analyse de la base de données de boîtes aux lettres Exchange. Cette fonctionnalité est uniquement disponible pour Microsoft Exchange Server 2007 ou version ultérieure avec le rôle serveur de boîte aux lettres ou serveur de transport Hub. Ce type d'analyse s'applique également à une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend un des rôles de serveur indiqués). Pour plus d'informations sur les rôles d'Exchange 2013, consultez Rôles Exchange Server 2013.

1.3.1 Protection de la base de données de boîtes aux lettres

L'analyse de boîtes aux lettres est déclenchée et contrôlée par le serveur Microsoft Exchange. Les messages stockés dans la base de données du serveur Microsoft Exchange Server sont analysés en continu. En fonction de la version de Microsoft Exchange Server, de la version de l'interface VSAPI et des paramètres définis par l'utilisateur, l'analyse peut être déclenchée dans l'un des cas suivants :

- lorsque l'utilisateur accède à sa messagerie, dans un client de messagerie par exemple (les messages sont toujours analysés avec la dernière base des signatures de virus) ;
- en arrière-plan, lorsque l'utilisation du serveur Microsoft Exchange Server est faible ;
- de manière proactive (en fonction de l'algorithme interne de Microsoft Exchange Server).

L'interface VSAPI est utilisée pour l'analyse antivirus et la protection basée sur les règles.

1.3.2 Protection du transport des messages

Le filtrage de messages au niveau du serveur SMTP est assuré par un plugin spécialisé. Dans Microsoft Exchange Server 2000 et 2003, ce plugin (*récepteur d'événements*) est enregistré sur le serveur SMTP dans le cadre des services IIS (Internet Information Services). Dans Microsoft Exchange Server 2007/2010, le plugin est enregistré en tant qu'agent de transport dans les rôles *Edge* ou *Hub* du serveur Microsoft Exchange.

Le filtrage au niveau du serveur SMTP effectué par un agent de transport offre une protection sous la forme de règles antivirus, antispam et définies par l'utilisateur. Contrairement au filtrage VSAPI, le filtrage au niveau du serveur SMTP est effectué avant l'arrivée des messages analysés dans la boîte aux lettres Microsoft Exchange Server.

1.3.3 Analyse de base de données à la demande

Comme l'exécution d'une analyse de base de données de messagerie complète peut entraîner une charge système indésirable, vous pouvez choisir quelles bases de données et quelles boîtes aux lettres analyser. Vous pouvez filtrer les cibles à analyser en spécifiant l'horodatage des messages à analyser afin de limiter l'impact sur les ressources système du serveur.

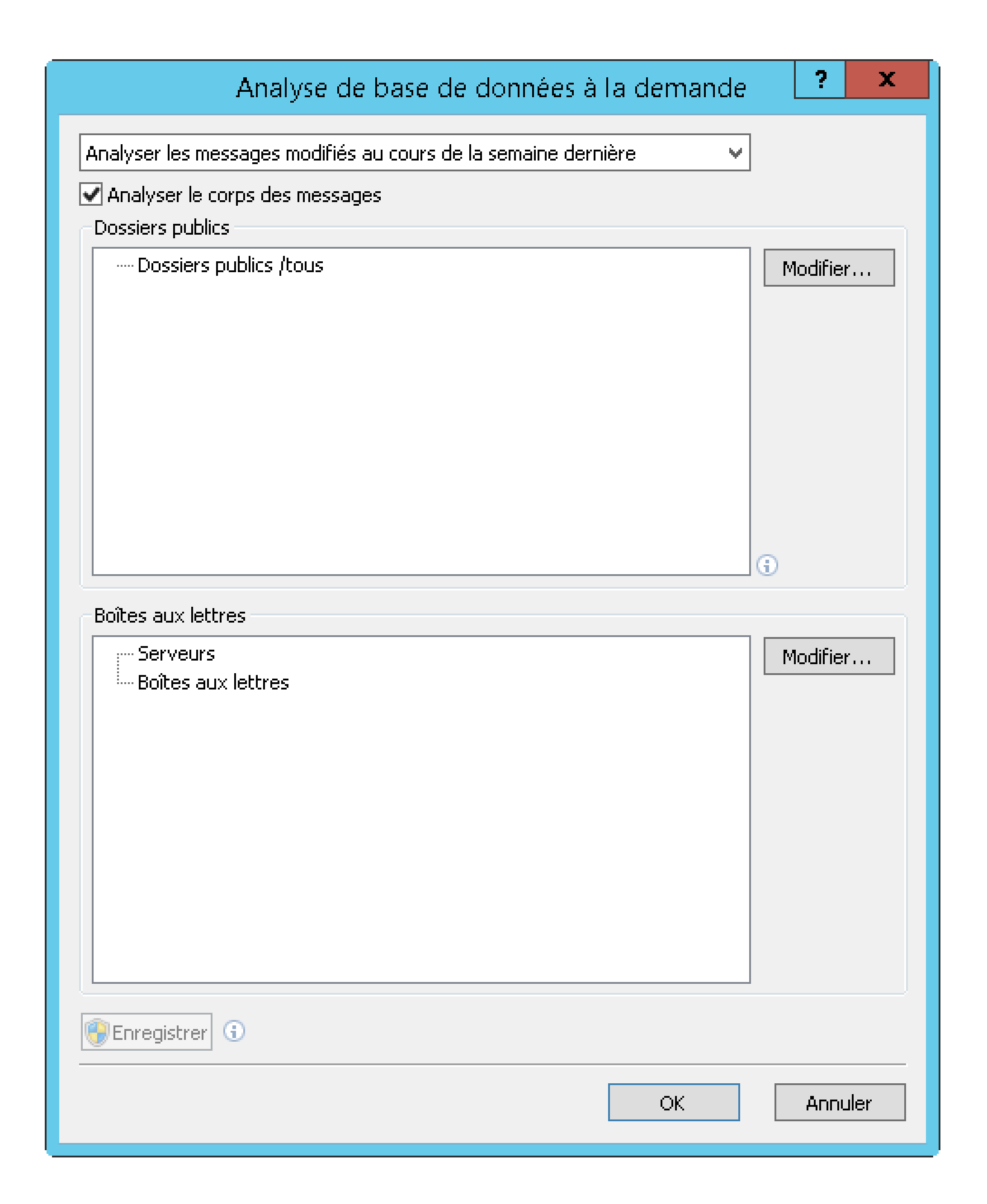
Les types d'élément suivants sont analysés dans les dossiers publics et les boîtes aux lettres des utilisateurs :

- Courrier électronique
- Publication
- Éléments de calendrier (réunions/rendez-vous)
- Tâches
- Contacts
- Journal

Vous pouvez utiliser la liste déroulante pour sélectionner les messages à analyser en fonction de leur horodatage (les messages modifiés au cours de la semaine dernière, par exemple). Vous avez également la possibilité d'analyser tous les messages, si cela s'avère nécessaire.

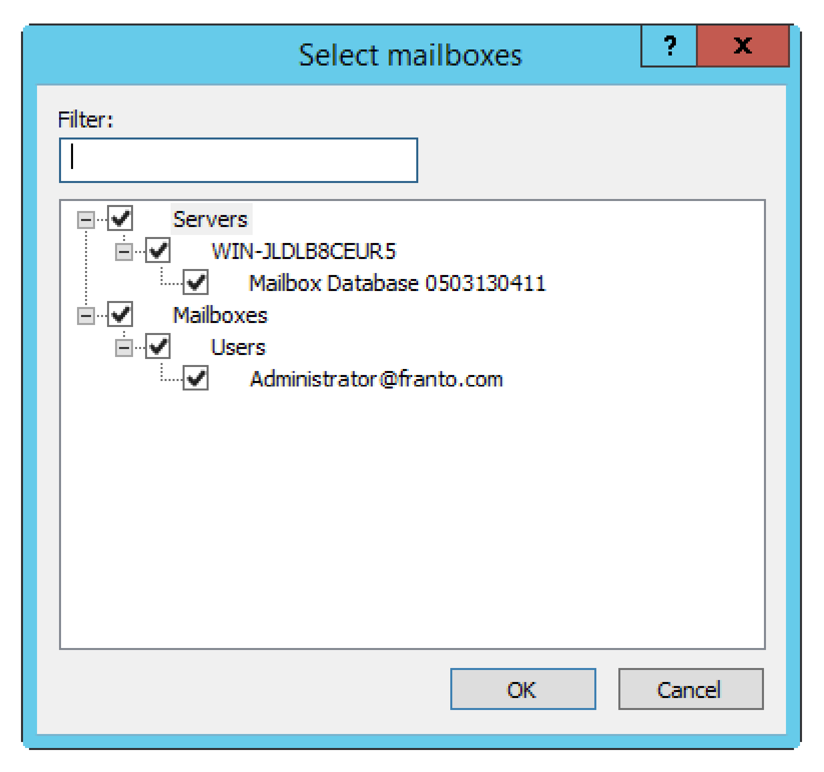
Cochez la case située en regard de l'option **Analyser le corps des messages** pour activer ou désactiver l'analyse du corps des messages.

Cliquez sur **Modifier** pour sélectionner le dossier public à analyser.



Analyse de base de données à la demande
?
Analyser les messages modifiés au cours de la semaine dernière
Analyser le corps des messages
Dossiers publics
Dossiers publics /tous
Modifier...
Boîtes aux lettres
Serveurs
Boîtes aux lettres
Modifier...
Enregistrer
OK
Annuler

Cochez les cases en regard des bases de données et des boîtes aux lettres du serveur à analyser. Le **filtrage** vous permet de retrouver rapidement les bases de données et les boîtes aux lettres, tout particulièrement si votre infrastructure Exchange contient un grand nombre de boîtes aux lettres.



Cliquez sur **Enregistrer** pour enregistrer les cibles à analyser et les paramètres dans le profil d'analyse à la demande.

1.4 Types de protection

Il existe trois types de protection :

- Protection antivirus
- Protection antispam
- Application des règles définies par l'utilisateur

1.4.1 Protection antivirus

La protection antivirus est l'une des fonctions de base d'ESET Mail Security. La protection antivirus vous prémunit des attaques contre le système en contrôlant les échanges de fichiers et de courrier, ainsi que les communications Internet. Si une menace comportant un code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant dans un premier temps, puis en la nettoyant, en la supprimant ou en lamettant en quarantaine.

1.4.2 Protection antispam

La protection antispam intègre plusieurs technologies (RBL, DNSBL, empreintes digitales, vérification de la réputation, analyse de contenu, filtre bayésien, règles, création manuelle de liste blanche/noire, etc.) afin d'optimiser la détection des menaces par courrier électronique. Le moteur d'analyse antispam génère la probabilité, exprimée sous forme de pourcentage (0 à 100) selon laquelle un message donné peut être un courrier indésirable.

ESET Mail Security peut également utiliser la méthode de mise en liste grise (désactivée par défaut) du filtrage du courrier indésirable. Cette méthode repose sur la spécification RFC 821 : le protocole SMTP étant considéré comme étant non fiable, chaque agent de transfert de message doit réessayer plusieurs fois de livrer un message électronique en cas de défaillance temporaire de livraison. La plupart des messages indésirables sont remis une seule fois à une liste importante d'adresses électroniques générée automatiquement. La mise en liste grise calcule une valeur de contrôle (hachage) pour l'adresse de l'expéditeur, l'adresse du destinataire et l'adresse IP de l'agent de transfert de message chargé de l'envoi. Si le serveur ne parvient pas à détecter la valeur de contrôle du triplet

dans sa base de données, il refuse le message et renvoie un code de défaillance temporaire (par exemple 451). Un serveur légitime essaie de renvoyer le message après une période définie qui peut être variable. La valeur de contrôle triplet est stockée dans la base de données des connexions vérifiées lors de la deuxième tentative, ce qui permet ensuite de transférer correctement tout autre message ayant les mêmes caractéristiques.

1.4.3 Application des règles définies par l'utilisateur

La protection basée sur les règles permet d'effectuer des analyses à l'aide de VSAPI et de l'agent de transport. L'interface utilisateur ESET Mail Security permet de créer différentes règles qui peuvent être combinées. Si une règle utilise plusieurs conditions, ces dernières sont liées à l'aide de l'opérateur logique AND. Par conséquent, la règle n'est exécutée que si toutes ses conditions sont remplies. Si plusieurs règles sont créées, l'opérateur logique OR est appliqué, ce qui signifie que le programme exécute la première règle dont les conditions sont remplies.

Dans la séquence d'analyse, la première technique utilisée est la mise en liste grise, si elle est activée. Les procédures suivantes utilisent toujours les techniques suivantes : protection basée sur des règles définies par l'utilisateur, suivie d'une analyse antivirus et enfin d'une analyse antispam.

1.5 Interface utilisateur

ESET Mail Security dispose d'une interface utilisateur graphique très intuitive. Elle permet d'accéder très facilement aux principales fonctions du programme.

Outre l'interface utilisateur principale, une **fenêtre Configuration avancée** est accessible depuis tous les emplacements du programme par l'intermédiaire de la touche F5.

Depuis la fenêtre Configuration avancée, vous pouvez configurer les paramètres et les options en fonction de vos besoins. Le menu situé à gauche se compose des catégories suivantes : . Certaines des catégories comportent des sous-catégories. Lorsque vous cliquez sur un élément (catégorie ou sous-catégorie) dans le menu de gauche, les paramètres correspondant à cet élément s'affichent dans le volet de droite.

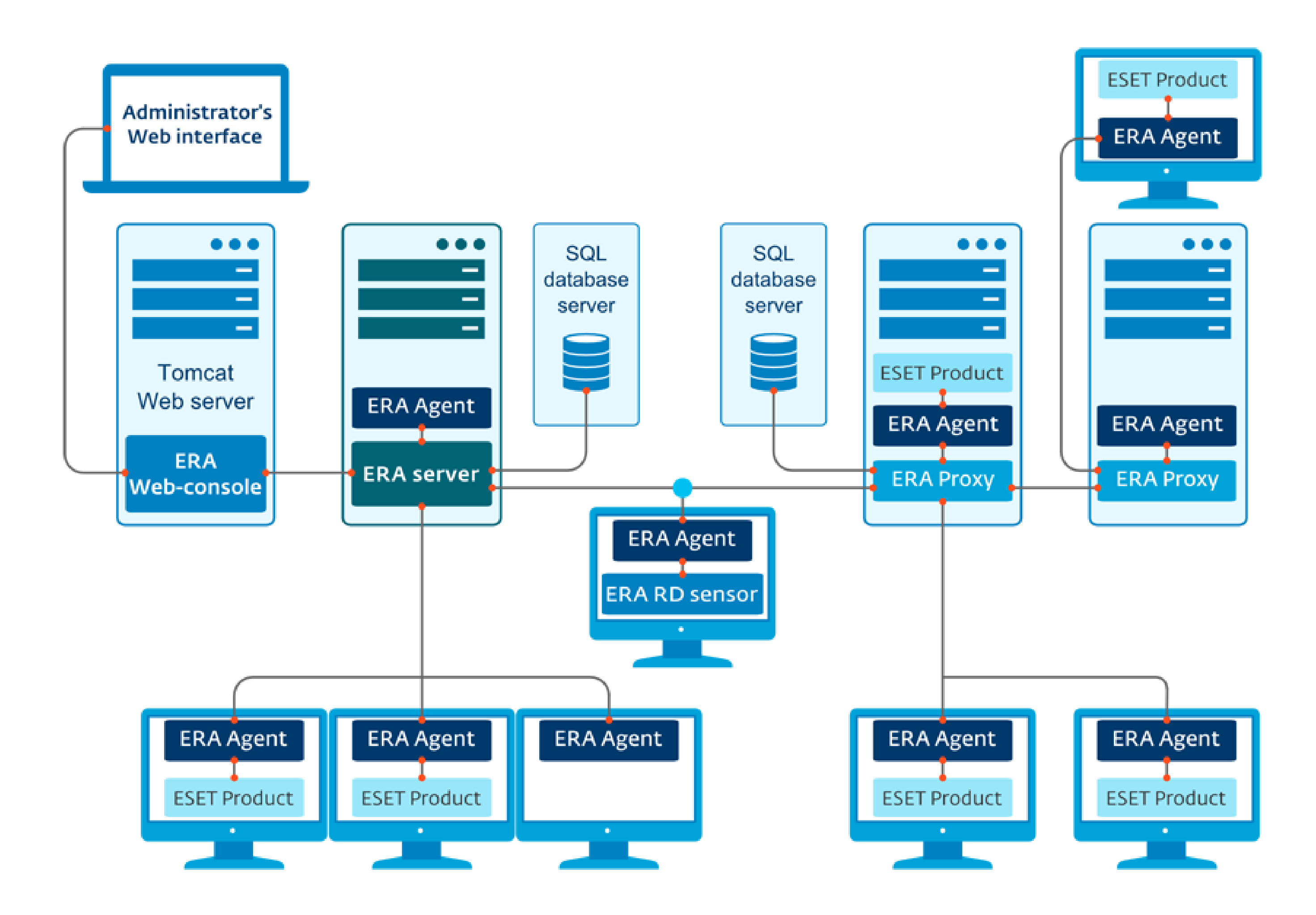
Pour plus d'informations sur l'interface utilisateur graphique, cliquez ici.

1.6 Gérés via ESET Remote Administrator

ESET Remote Administrator (ERA) est une application qui permet de gérer les produits ESET de manière centralisée dans un environnement réseau. Le système de gestion des tâches ESET Remote Administrator permet d'installer les solutions de sécurité ESET sur des ordinateurs distants et de réagir rapidement face aux nouveaux problèmes et menaces. ESET Remote Administrator n'offre pas de protection contre les codes malveillants ; le produit repose sur la présence de la solution de sécurité ESET sur chaque client.

Les solutions de sécurité ESET prennent en charge les réseaux qui comprennent plusieurs types de plateformes. Votre réseau peut comprendre une combinaison de systèmes d'exploitation Microsoft, Linux et OS X et de systèmes d'exploitation qui s'exécutent sur des périphériques mobiles (téléphones mobiles et tablettes).

L'illustration suivante montre un exemple d'architecture pour un réseau protégé par les solutions de sécurité ESET gérées par ERA :



REMARQUE : pour plus d'informations sur ERA, reportez-vous à l'aide en ligne d'ESET Remote Administrator.

1.6.1 ERA Server

ESET Remote Administrator Server est un composant principal d'ESET Remote Administrator. Il s'agit de l'application d'exécution qui traite toutes les données reçues des clients se connectant à cette dernière (par le biais d'ERA Agent). ERA Agent facilite la communication entre le client et le serveur. Les données (journaux clients, configuration, réplication de l'agent et autres) sont stockées dans une base de données. Pour traiter correctement les données, ERA Server requiert une connexion stable à un serveur de base de données. Pour optimiser les performances, nous vous conseillons d'installer le serveur ERA et la base de données sur des serveurs distincts. L'ordinateur sur lequel ERA Server est installé doit être configuré pour accepter toutes les connexions Agent/Proxy/RD Sensor qui sont vérifiées à l'aide de certificats. Après l'installation d'ERA Server, vous pouvez ouvrir ERA Web Console qui se connecte à ERA Server (comme le montre le diagramme). À partir de la console Web, toutes les opérations d'ERA Server sont effectuées lors de la gestion des solutions de sécurité ESET dans votre environnement.

1.6.2 Console Web

ERA Web Console est une application dotée d'une interface utilisateur Web qui présente les données d'ERA Server et permet de gérer les solutions de sécurité ESET dans votre environnement. La console Web est accessible à l'aide d'un navigateur. Elle affiche une vue d'ensemble de l'état des clients sur le réseau et peut être utilisée pour déployer à distance les solutions ESET sur des ordinateurs non gérés. Si vous choisissez de rendre accessible le serveur Web à partir d'Internet, vous pouvez alors utiliser ESET Remote Administrator à partir de la plupart des emplacements ou périphériques disposant d'une connexion Internet active.

Voici le tableau de bord de la console Web :



La barre supérieure de la console Web contient l'outil **Recherche rapide**. Dans le menu déroulant, sélectionnez **Nom de l'ordinateur**, **Adresse IPv4/IPv6** ou **Nom de la menace**, saisissez votre chaîne de recherche dans le champ de texte, puis cliquez sur le symbole de loupe ou appuyez sur la touche **Entrée** pour lancer la recherche. Vous êtes alors redirigé vers la section Groupes qui affiche les résultats de la recherche (client ou liste de clients). Tous les clients sont gérés par le biais de la console Web. Vous pouvez avoir accès à la console à l'aide des périphériques et des navigateurs les plus courants.

REMARQUE : pour plus d'informations, reportez-vous à l'aide en ligne d'ESET Remote Administrator.

1.6.3 Agent

ERA Agent est un composant essentiel du produit ESET Remote Administrator. Un produit ESET sur une machine client (ESET Endpoint security pour Windows, par exemple) communique avec ERA Server par le biais de l'agent. Cette communication permet de gérer les produits ESET sur tous les clients distants à partir d'un seul emplacement. L'Agent collecte les informations sur le client et les envoie au serveur. Si le serveur envoie une tâche destinée au client, celle-ci est envoyée à l'Agent qui l'envoie à son tour au client. Toutes les communications réseau ont lieu entre l'Agent et la partie supérieure du réseau ERA, à savoir le serveur et le proxy.

ESET Agent utilise l'une des trois méthodes suivantes pour se connecter au serveur :

1. L'Agent du client est directement connecté au serveur.
2. L'Agent du client est connecté par le biais d'un proxy connecté au serveur.
3. L'Agent du client est connecté au serveur par le biais de plusieurs proxys.

ESET Agent communique avec les solutions ESET installées sur un client, collecte les informations des programmes du client et transmet les informations de configuration reçues du serveur au client.

ℹ **REMARQUE :** ESET Proxy possède son propre Agent qui gère toutes les tâches de communication entre les clients, les autres proxys et le serveur.

1.6.4 RD Sensor

RD (Rogue Detection) Sensor est un outil de recherche des ordinateurs sur le réseau. RD Sensor est un composant d'ESET Remote Administrator qui est conçu pour détecter les ordinateurs sur votre réseau. Il offre un moyen pratique d'ajouter de nouveaux ordinateurs à ESET Remote Administrator sans avoir à les rechercher et à les ajouter manuellement. Tous les ordinateurs détectés sur votre réseau sont affichés dans la console Web. À ce stade, vous pouvez effectuer d'autres actions sur chaque ordinateur client.

RD Sensor est un écouteur passif qui détecte les ordinateurs qui se trouvent sur le réseau et envoie des informations sur ces derniers à ERA Server. ERA Server évalue ensuite si les ordinateurs trouvés sur le réseau sont inconnus ou déjà gérés.

1.6.5 Proxy

ERA Proxy est un autre composant d'ESET Remote Administrator qui a un double objectif. Dans le cas d'un réseau d'entreprise de taille moyenne qui comprend de nombreux clients (10 000 clients ou plus), ERA Proxy peut servir à répartir la charge entre plusieurs ERA Proxy, et décharger ainsi le serveur principal ERA Server. L'autre avantage du proxy ERA, c'est que vous pouvez l'utiliser dans le cadre d'une connexion de qualité médiocre à une filiale distante. Cela signifie qu'ERA Agent sur chaque client ne se connecte pas directement à ERA Server, mais par le biais d'ERA Proxy qui se trouve sur le même réseau local de la filiale. Il libère ainsi la liaison de la filiale. ERA Proxy accepte les connexions de tous les ERA Agents locaux, regroupe leurs données et les télécharge sur le serveur principal ERA Server (ou un autre ERA Proxy). Votre réseau peut ainsi prendre en charge davantage de clients sans compromettre les performances du réseau et des requêtes de base de données.

Selon votre configuration réseau, le proxy ERA peut se connecter à un autre proxy ERA, puis au serveur ERA.

Pour qu'ERA Proxy fonctionne correctement, l'ordinateur hôte sur lequel vous avez installé ERA Proxy doit disposer d'un ESET Agent et être connecté au niveau supérieur (ERA Server ou ERA Proxy supérieur, le cas échéant) du réseau.

ℹ **REMARQUE :** pour obtenir un exemple de scénario de déploiement d'ERA Proxy, reportez-vous à l'aide en ligne d'ESET Remote Administrator.

2. Configuration système

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2003 (x86 et x64)
- Microsoft Windows Server 2003 R2 (x86 et x64)
- Microsoft Windows Server 2008 (x86 et x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Versions de Microsoft Exchange Server 2003 prises en charge :

- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU4 (SP1), CU5, CU6, CU7, CU8
- Microsoft Exchange Server 2016

La configuration matérielle dépend de la version du système d'exploitation utilisée. Il est recommandé de prendre connaissance de la documentation Microsoft Windows Server pour plus d'informations sur la configuration matérielle.

3. Installation

Après l'achat d'ESET Mail Security, le programme d'installation peut être téléchargé à partir du site web d'ESET (www.eset.com) sous forme de package .msi.

Veuillez noter que vous devez exécuter le programme d'installation avec le compte Administrateur intégré. Aucun autre utilisateur, même membre du groupe Administrateurs, ne disposera de droits d'accès suffisants. Vous devez donc utiliser un compte Administrateur intégré dans la mesure où vous ne parviendrez à effectuer l'installation avec aucun autre compte qu'Administrateur.

Il est possible d'exécuter le programme d'installation de deux façons :

- Vous pouvez vous connecter localement à l'aide des informations d'identification du compte Administrateur et simplement exécuter le programme d'installation
- Vous pouvez être connecté avec un autre compte d'utilisateur, mais vous devez ouvrir l'invite de commande avec Exécuter en tant que... et taper les informations d'identification du compte Administrateur pour que cmd s'exécute en tant qu'Administrateur, puis taper la commande pour exécuter le programme d'installation (par exemple, msiexec /i mais vous devez remplacer par le nom de fichier précis du programme d'installation msi que vous avez téléchargé)

Une fois que vous avez lancé le programme d'installation et accepté les termes du Contrat de Licence Utilisateur Final (CLUF), l'assistant d'installation vous guide tout au long de la procédure d'installation. Si vous refusez les termes du Contrat de Licence, l'assistant s'interrompt.

Terminer
Il s'agit du type d'installation recommandé. Il installe toutes les fonctionnalités d'ESET Mail Security. Lorsque vous choisissez ce type d'installation, vous devez uniquement spécifier les dossiers dans lesquels installer le produit. Vous pouvez également accepter les dossiers d'installation par défaut prédéfinis (recommandé). Le programme d'installation installe ensuite automatiquement toutes les fonctionnalités du programme.

Personnalisé
L'installation personnalisée vous permet de choisir les fonctionnalités du programme ESET Mail Security à installer sur votre système. Vous sélectionnez les fonctionnalités/composants à installer dans une liste classique.

Outre l'assistant d'installation, vous pouvez choisir d'installer ESET Mail Security de manière silencieuse par le biais d'une ligne de commande. Ce type d'installation ne demande aucune intervention de l'utilisateur, contrairement à l'assistant d'installation. Il s'avère utile pour automatiser ou simplifier l'installation. Ce type d'installation est également appelé installation sans assistance car il ne demande aucune action de la part de l'utilisateur.

Installation silencieuse/sans assistance
Effectuez l'installation à l'aide de la ligne de commande : `msiexec /i <nom_package> /qn /l*xv msi.log`

i **REMARQUE** : Il est fortement recommandé, dans la mesure du possible, d'installer ESET Mail Security sur un système d'exploitation récemment installé et configuré. Toutefois, si vous n'avez pas besoin de l'installer sur un système existant, la meilleure solution consiste à désinstaller la version antérieure de ESET Mail Security, de redémarrer le serveur et d'installer ensuite la nouvelle version de ESET Mail Security.

i **REMARQUE**: si vous avez déjà utilisé un autre logiciel antivirus tiers sur votre système, nous vous recommandons de le désinstaller complètement avant d'installer ESET Mail Security. Vous pouvez pour cela utiliser ESET AV Remover qui simplifie la désinstallation.

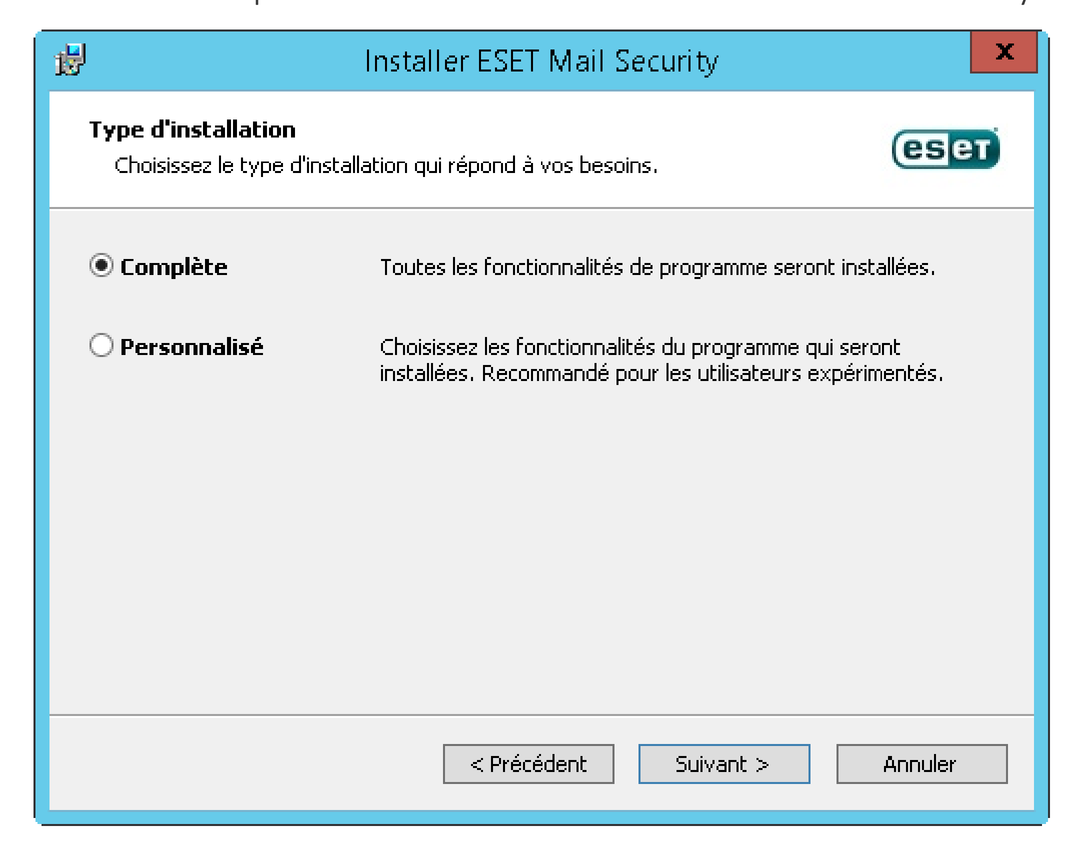
3.1 Étapes d'installation d'ESET Mail Security

Suivez ces étapes pour installer ESET Mail Security à l'aide de l'assistant d'installation :



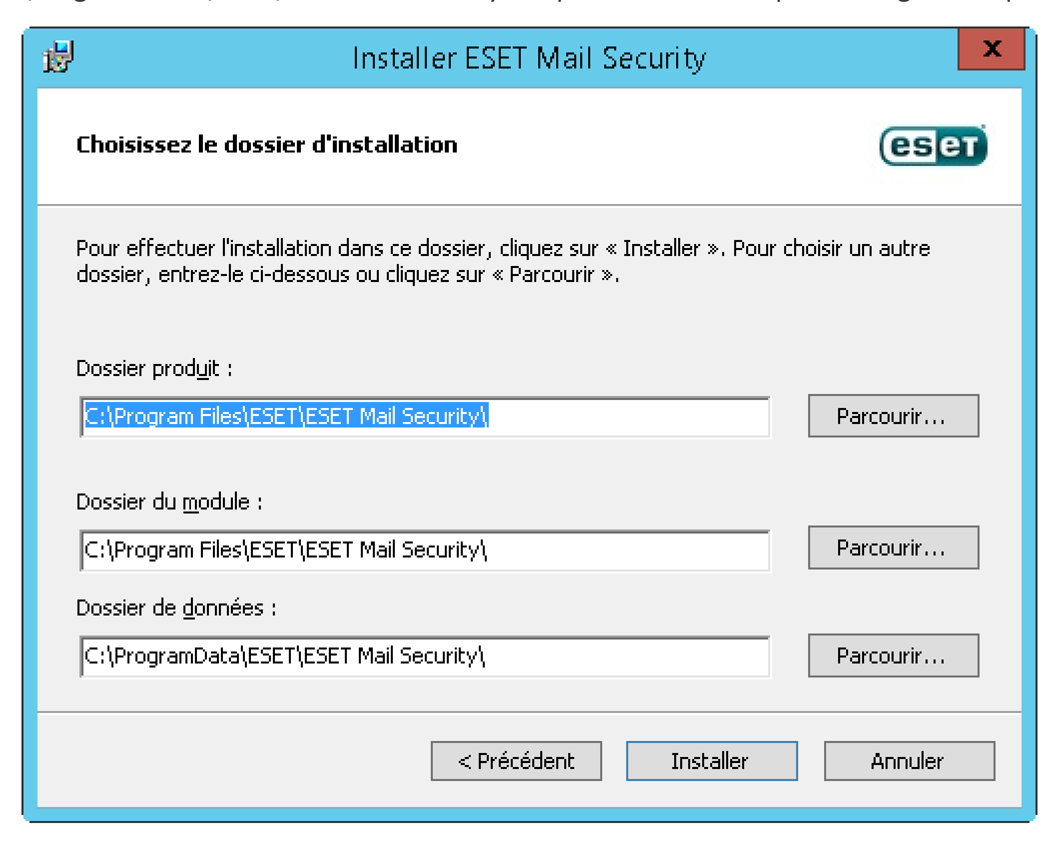
Une fois les termes du CLUF acceptés, sélectionnez l'un des types d'installation suivants :

- **Complète** : permet d'installer toutes les fonctionnalités d'ESET Mail Security. Il s'agit du type d'installation recommandé.
- **Personnalisée** : permet de sélectionner les fonctionnalités d'ESET Mail Security à installer sur votre système.



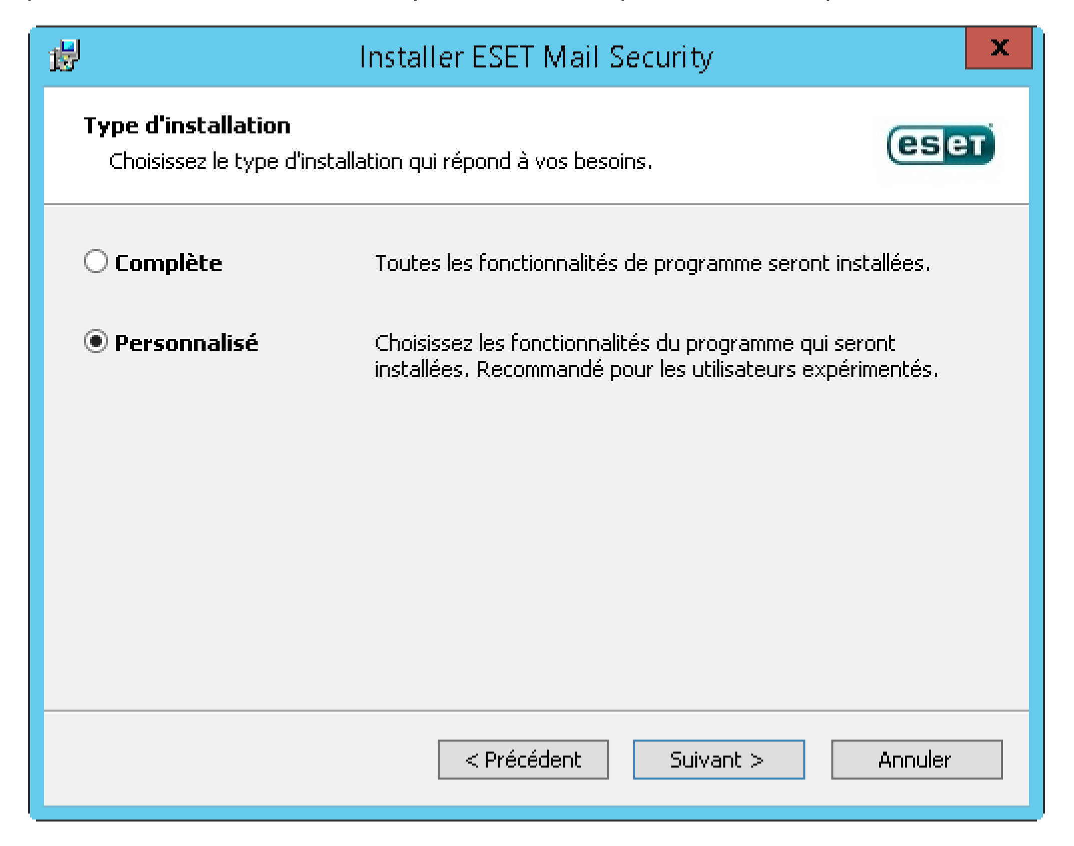
Installation complète :

Également appelée installation intégrale. Tous les composants ESET Mail Security sont installés. Vous êtes invité à sélectionner l'emplacement d'installation d'ESET Mail Security. Par défaut, le programme s'installe dans le dossier C:\Program Files\ESET\ESET Mail Security. Cliquez sur **Parcourir** pour changer d'emplacement (non recommandé).



Installation personnalisée :

Ce type d'installation permet de sélectionner les fonctionnalités à installer. Il s'avère utile lorsque vous souhaitez personnaliser ESET Mail Security et installer uniquement les composants dont vous avez besoin.

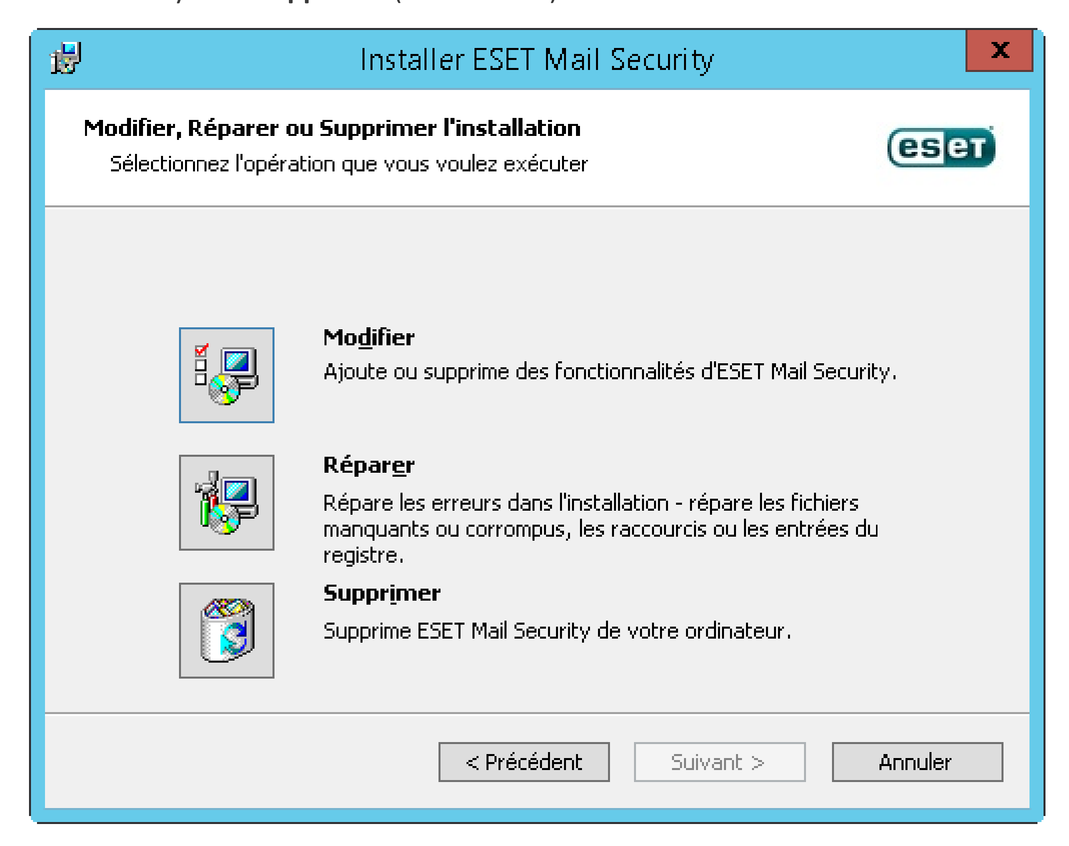


Vous pouvez ajouter ou supprimer des composants inclus dans l'installation. Pour ce faire, exécutez le fichier d'installation .msi que vous avez utilisé lors de l'installation initiale ou accédez à **Programmes et fonctionnalités**

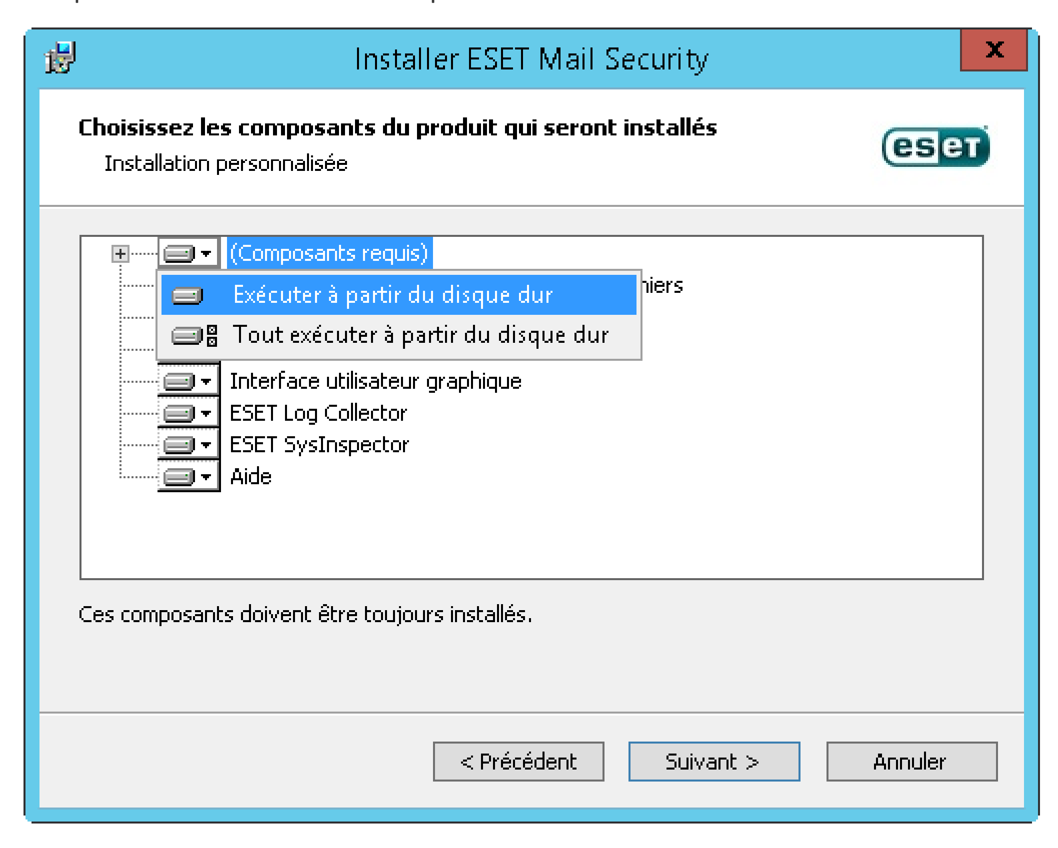
(accessible à partir du Panneau de configuration Windows), cliquez avec le bouton droit sur ESET Mail Security, puis sélectionnez **Modifier**. Suivez ces étapes pour ajouter ou supprimer des composants.

Procédure de modification des composants (Ajouter/supprimer), réparation et suppression :

Trois options sont disponibles : Vous pouvez **modifier** les composants installés, **réparer** votre installation d'ESET Mail Security ou la **supprimer** (désinstaller) entièrement.



Si vous sélectionnez l'option **Modifier**, la liste des composants disponibles s'affiche. Choisissez les composants à ajouter ou à supprimer. Vous pouvez ajouter/supprimer simultanément plusieurs composants. Cliquez sur le composant et sélectionnez une option dans le menu déroulant :

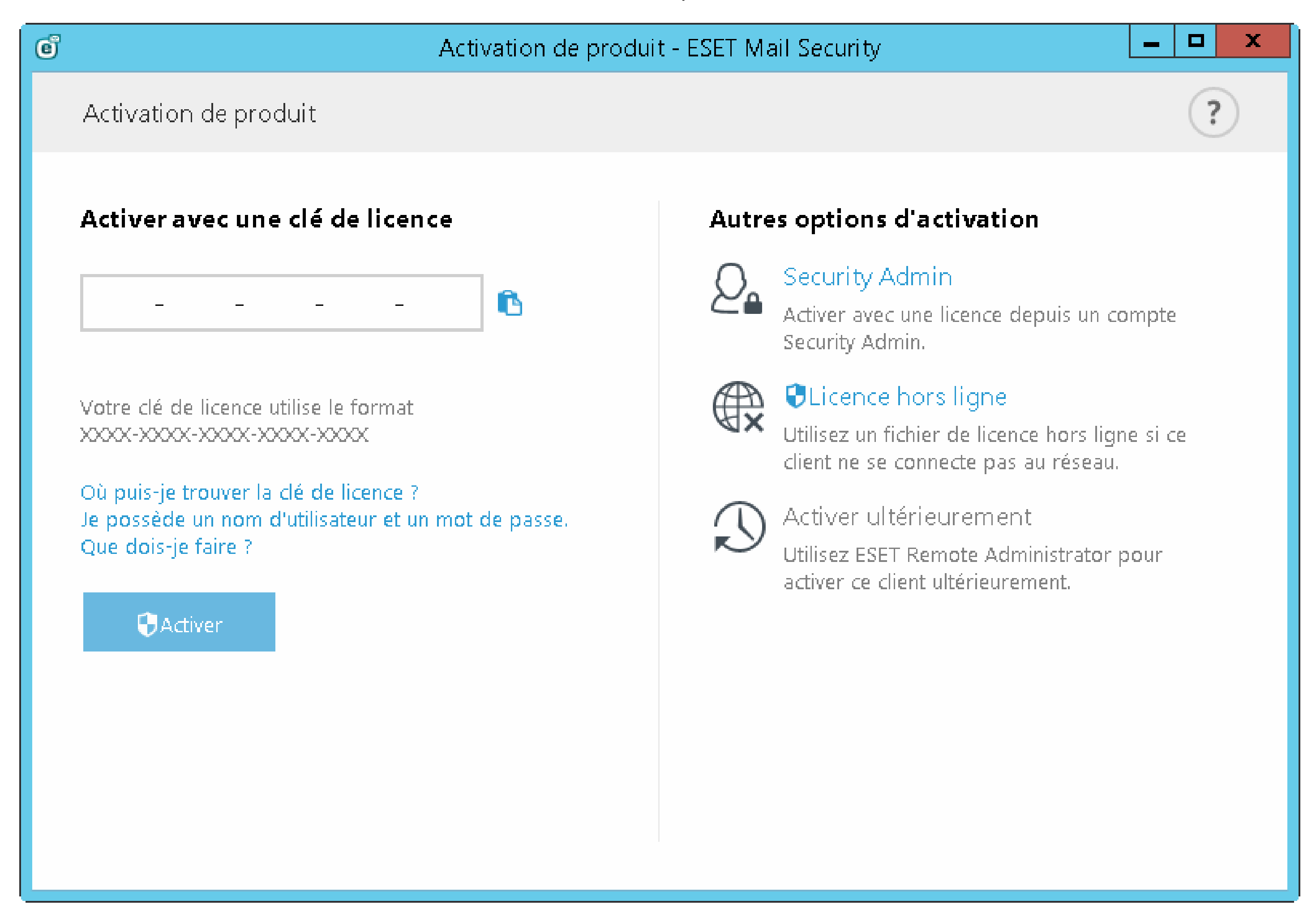


Après avoir sélectionné une option, cliquez sur **Modifier** pour effectuer les modifications.

REMARQUE : vous pouvez modifier à tout moment les composants installés en exécutant le programme d'installation. Pour la plupart des composants, un redémarrage du serveur n'est pas nécessaire pour prendre en compte la modification. L'interface utilisateur redémarre et seuls les composants que vous avez choisi d'installer sont visibles. Pour les composants qui nécessitent un redémarrage du serveur, Windows Installer vous demande de redémarrer le serveur. Les nouveaux composants seront disponibles une fois que le serveur sera en ligne.

3.2 Activation du produit

Une fois l'installation terminée, vous êtes invité à activer le produit.



Sélectionnez l'une des méthodes disponibles pour activer ESET Mail Security. Pour plus d'informations, reportez-vous à la section Comment activer ESET Mail Security.

Une fois ESET Mail Security activé, la fenêtre principale du programme s'ouvre et affiche l'état actuel dans la page Supervision.

La fenêtre principale du programme affiche également des notifications sur d'autres éléments tels que les mises à jour du système (Windows Update) ou les mises à jour de la base des signatures de virus. Lorsque vous avez répondu à tous ces points, l'état de surveillance devient vert et indique **Protection maximale**.

3.3 Terminal Server

Si vous installez ESET Mail Security sur un serveur Windows Server agissant comme Terminal Server, vous souhaiterez peut-être désactiver l'interface utilisateur graphique ESET Mail Security afin d'empêcher son démarrage à chaque connexion de l'utilisateur. Reportez-vous à la section Désactivation de l'interface utilisateur graphique sur Terminal Server pour accéder aux étapes de désactivation.

3.4 ESET AV Remover

Pour supprimer/désinstaller un logiciel antivirus tiers de votre système, nous vous recommandons d'utiliser ESET AV Remover. Pour ce faire, procédez comme suit :

1. Téléchargez ESET AV Remover à partir du site Web ESET Page de téléchargement des utilitaires.
2. Cliquez sur **I accept, start search** (J'accepte, lancer la recherche) pour accepter le contrat de l'utilisateur final (CLUF) et démarrer la recherche sur le système.
3. Cliquez sur **Launch uninstaller** (Lancer le programme de désinstallation) pour supprimer le logiciel antivirus installé.

Pour obtenir la liste des logiciels antivirus tiers qu'ESET AV Remover peut supprimer, consultez cet article de la base de connaissances.

3.5 Mise à niveau vers une version plus récente

Les nouvelles versions d'ESET Mail Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne peuvent pas résoudre. Il est possible d'effectuer une mise à niveau à partir d'anciennes versions d'ESET Mail Security (versions 4.5 et antérieure), même s'il s'agit d'une mise à niveau vers une architecture différente. Vous disposez de deux méthodes pour effectuer la mise à niveau vers une version plus récente :

- Manuellement, en téléchargeant la nouvelle version et en l'installant sur la version existante. Exécutez le programme d'installation et effectuez une installation de la manière habituelle. ESET Mail Security transfère automatiquement la configuration existante, avec toutefois quelques exceptions (voir la remarque ci-dessous).
- À distance, dans un environnement réseau, via ESET Remote Administrator.

Important : certaines exceptions s'appliquent lors de la mise à niveau : tous les paramètres ne sont pas conservés, notamment les règles. En effet, les règles ont été entièrement reconçues dans ESET Mail Security 6 avec une approche différente. Les règles des versions précédentes d'ESET Mail Security ne sont pas compatibles avec celles d'ESET Mail Security version 6. Il est recommandé de configurer manuellement les règles, ce qui peut également vous aider.

Vous trouverez ci-dessous la liste des paramètres qui sont conservés des versions précédentes d'ESET Mail Security:

- Configuration générale d'ESET Mail Security
- Paramètres de protection antispam
  - Tous les paramètres identiques dans les versions précédentes ; les nouveaux paramètres utilisent les valeurs par défaut.
  - Listes blanches et noires

REMARQUE : une fois le produit ESET Mail Security mis à niveau, il est recommandé d'examiner tous les paramètres pour vérifier qu'ils sont correctement configurés et qu'ils répondent à vos besoins.

3.6 Rôles Exchange Server - Comparaison entre Edge et Hub

Par défaut, les fonctionnalités antispam sont désactivées sur les serveurs de transport Edge et Hub. Cette configuration est à privilégier dans une organisation Exchange avec serveur de transport Edge. Il est recommandé que le serveur de transport Edge exécute le filtrage antispam ESET Mail Security sur les messages avant leur transmission dans l'organisation Exchange.

Le rôle Edge reste toutefois l'emplacement privilégié de l'analyse antispam, car il permet à ESET Mail Security de rejeter les courriers indésirables dans les premières phases du processus sans charger inutilement les couches réseau. Dans cette configuration, les messages entrants sont filtrés par ESET Mail Security sur le serveur de transport Edge, afin qu'ils puissent être envoyés en toute sécurité au serveur de transport Hub sans nécessiter de filtrage supplémentaire.

Si votre organisation n'utilise pas de serveur de transport Edge et ne dispose que d'un serveur de transport Hub, il est recommandé d'activer les fonctionnalités antispam de ce dernier qui reçoit via SMTP les messages entrants provenant d'Internet.

3.7 Rôles Exchange Server 2013

L'architecture d'Exchange Server 2013 est différente de celle des versions précédentes de Microsoft Exchange. Depuis la version Exchange 2013, la mise à jour cumulative CU4 (qui correspond en fait au SP1 d'Exchange 2013) a réintroduit le rôle de serveur de transport Edge.

Si vous comptez protéger Microsoft Exchange 2013 avec ESET Mail Security, veillez à installer ESET Mail Security sur un système exécutant Microsoft Exchange 2013 avec le rôle de serveur de messagerie ou de transport Edge.

Il existe toutefois une exception si vous envisagez d'installer ESET Mail Security sur Windows SBS (Small Business Server) ou si Microsoft Exchange 2013 est installé sur un serveur avec plusieurs rôles. Dans ce cas, tous les rôles Exchange s'exécutent sur un même serveur. Par conséquent, ESET Mail Security offre une protection complète qui comprend les serveurs de messagerie.

Si vous installez ESET Mail Security sur un système exécutant uniquement le rôle de serveur d'accès au client (serveur CAS dédié), les fonctionnalités les plus importantes de ESET Mail Security sont désactivées, notamment celles de serveur de messagerie. Dans ce cas, seuls la protection en temps réel du système de fichiers et certains composants appartenant à la protection de l'ordinateur fonctionnent. Les serveurs de messagerie ne sont donc pas protégés. Pour cette raison, il n'est pas recommandé d'installer ESET Mail Security sur un serveur avec le rôle de serveur d'accès au client. Cela ne s'applique pas à Windows SBS (Small Business Server) et Microsoft Exchange avec plusieurs rôles sur un même serveur, comme indiqués plus haut.

i **REMARQUE**: en raison des restrictions techniques de Microsoft Exchange 2013, ESET Mail Security ne prend pas en charge le rôle de serveur d'accès au client (CAS). Cela ne s'applique pas à Windows SBS (Small Business Server) et Microsoft Exchange 2013 installé sur un serveur avec tous les rôles de serveur. Dans ce cas, vous pouvez exécuter ESET Mail Security avec le rôle de serveur d'accès au client sur le serveur, car le serveur de messagerie et le serveur de transport Edge sont protégés.

3.8 Connecteur POP3 et protection antispam

Les versions de Microsoft Windows Small Business Server (SBS) contiennent un connecteur POP3 intégré natif qui permet au serveur de récupérer les messages électroniques des serveurs POP3 externes. La mise en œuvre de ce connecteur POP3 natif de Microsoft varie selon la version de Microsoft Windows Small Business Server.

ESET Mail Security prend en charge le connecteur POP3 de Microsoft SBS, à condition qu'il soit configuré correctement. Les messages téléchargés via le connecteur POP3 de Microsoft sont analysés pour rechercher la présence de courrier indésirable. La protection antispam de ces messages est possible, car le connecteur POP3 transfère les messages électroniques d'un compte POP3 vers Microsoft Exchange Server via SMTP.

ESET Mail Security a été testé avec des services de messagerie courants, tels que **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** et **gmx.de**, sur les systèmes SBS suivants :

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

Important : si vous utilisez le connecteur POP3 intégré de Microsoft SBS et si tous les messages électroniques sont analysés pour rechercher la présence de courrier électronique, accédez à Configuration avancée, **Serveur** > **Protection du transport des messages** > Paramètres avancés. Pour le paramètre **Analyser également les messages reçus des connexions authentifiées ou internes**, sélectionnez **Analyser par protection antivirus et antispyware** dans la liste déroulante. La protection antispam est ainsi assurée pour les messages récupérés des comptes POP3.

Vous pouvez également utiliser un connecteur POP3 tiers tel que P3SS (au lieu du connecteur POP3 intégré de Microsoft SBS). ESET Mail Security a été testé sur les systèmes suivants (avec le connecteur P3SS récupérant les messages de **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** et **gmx.de**) :

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 avec Exchange Server 2007
- Microsoft Windows Server 2008 R2 avec Exchange Server 2010
- Microsoft Windows Server 2012 R2 avec Exchange Server 2013

4. Guide du débutant

Ce chapitre présente ESET Mail Security, les principaux éléments du menu, les fonctionnalités et les paramètres de base.

4.1 Interface utilisateur

La fenêtre principale d'ESET Mail Security est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Les différentes sections du menu principal sont décrites ci-dessous :

Supervision - Fournit des informations sur l'état de protection d'ESET Mail Security, la validité de la licence, la dernière mise à jour de la base des signatures de virus, les statistiques et les informations système.

Fichiers journaux - Permettent d'accéder aux fichiers journaux qui contiennent des informations sur tous les événements importants du programme qui se sont produits. Ces fichiers présentent les menaces détectées, ainsi que d'autres événements concernant la sécurité.

Analyse - Permet de configurer et de lancer l'analyse du stockage, l'analyse intelligente, l'analyse personnalisée ou l'analyse de supports amovibles. Vous pouvez également répéter la dernière analyse effectuée.

Mise à jour - Affiche des informations sur la base des signatures de virus et vous informe lorsqu'une mise à jour est disponible. L'activation du produit peut également être effectuée depuis cette section.

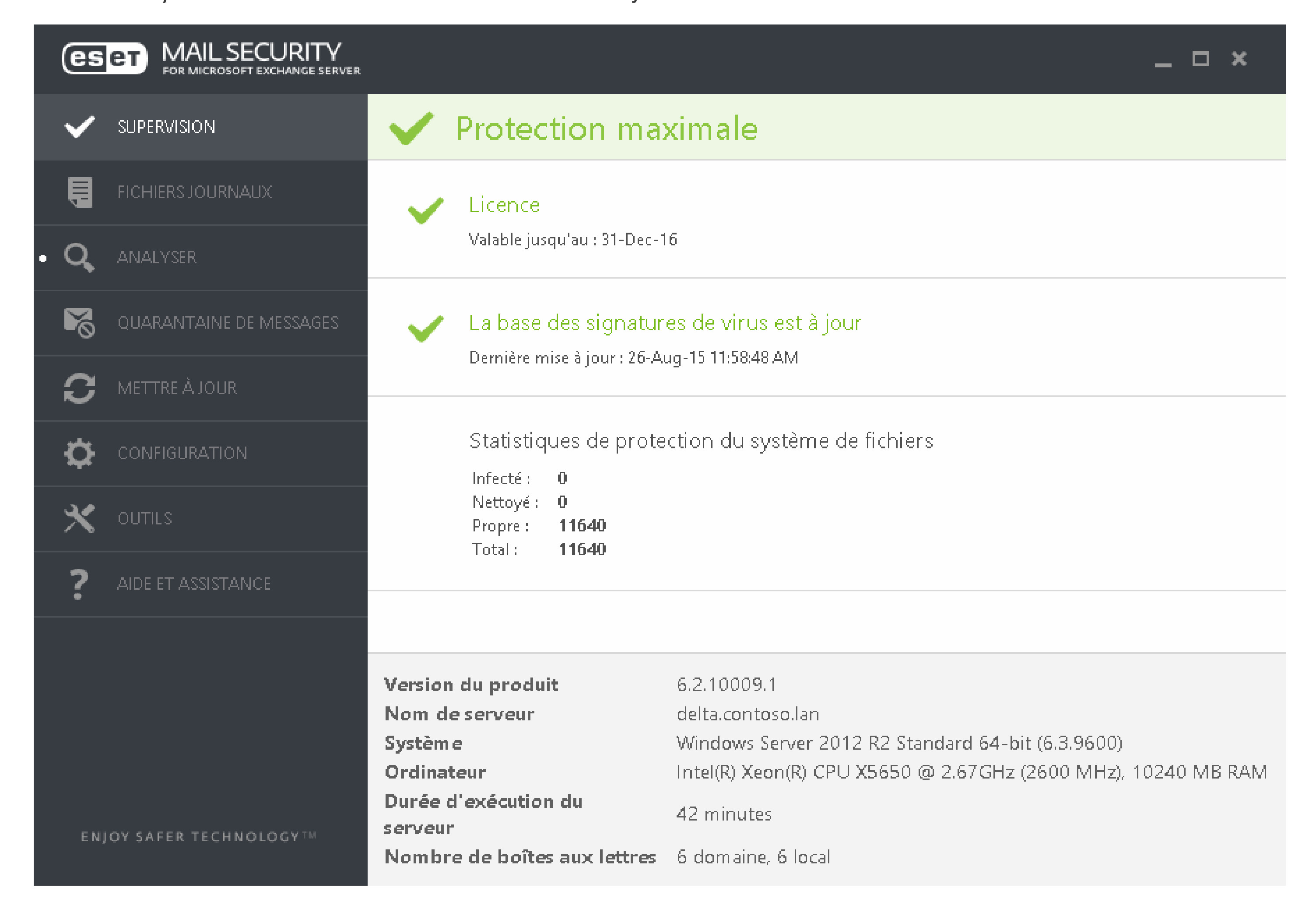
Configuration - Vous pouvez ajuster les paramètres de sécurité du serveur et de l'ordinateur.

Outils - Fournit des informations supplémentaires sur votre système et sur la protection, outre les outils qui permettent de mieux gérer votre sécurité. La section Outils comprend les éléments suivants : Processus en cours, Surveiller l'activité, ESET Log Collector, statistiques de protection, Cluster, ESET Shell, ESET SysInspector, ESET SysRescue Live pour créer un CD ou un stockage USB de secours, et Planificateur. Vous pouvez également soumettre un échantillon pour analyse et consulter la quarantaine.

Aide et assistance - Permet d'accéder aux fichiers d'aide, à la base de connaissances ESET et à d'autres outils d'assistance. Des liens sont également proposés pour ouvrir une requête auprès du service client et pour accéder à des informations sur l'activation du produit.

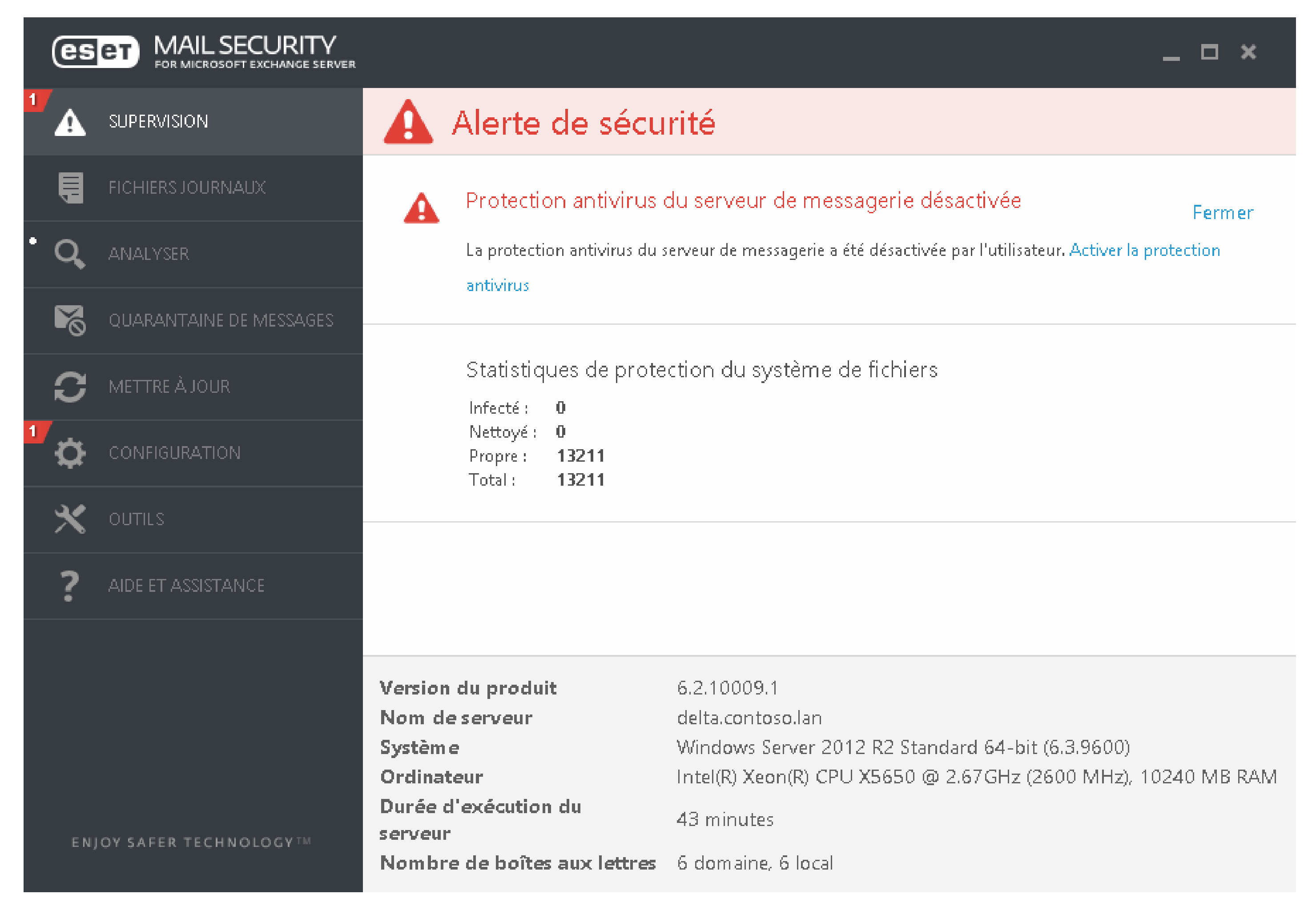
L'écran **État de la protection** vous informe sur le niveau actuel de protection de l'ordinateur. L'icône verte d'état **Protection maximale** indique qu'une protection maximale est assurée.

La fenêtre d'état contient également des liens rapides vers les fonctionnalités fréquemment utilisées dans ESET Mail Security et des informations sur la dernière mise à jour.



Que faire lorsque le programme ne fonctionne pas correctement ?

Une coche verte s'affiche en regard des modules qui fonctionnent correctement. Un point d'exclamation rouge ou une icône de notification orange s'affiche à côté des modules qui ne fonctionnent pas correctement. Des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état d'un module, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.



L'icône rouge indique des problèmes critiques ; la protection maximale de votre ordinateur n'est pas assurée. Cet état s'affiche dans les cas suivants :

- **Protection antivirus et antispyware désactivée** - Vous pouvez réactiver la protection antivirus et antispyware en cliquant sur **Activer la protection en temps réel** dans le volet **État de la protection** ou sur **Activer la protection antivirus et antispyware** dans le volet **Configuration** de la fenêtre principale du programme.
- Vous utilisez une base des signatures de virus obsolète.
- Le produit n'est pas activé.
- **Votre licence a expiré** - Cette information est indiquée par l'icône d'état de protection qui devient rouge. Le programme ne peut plus effectuer de mise à jour après expiration de la licence. Nous vous recommandons de suivre les instructions de la fenêtre d'alerte pour renouveler la licence.

L'icône orange indique que votre produit ESET nécessite votre attention en raison d'un problème non critique. Les raisons possibles sont les suivantes :

- **La protection de l'accès Web est désactivée** - Vous pouvez réactiver la protection de l'accès Web en cliquant sur la notification de sécurité, puis sur **Activer la protection de l'accès Web**.

- **Votre licence va arriver prochainement à expiration** - Cette information est donnée par l'icône d'état de protection qui affiche un point d'exclamation. Après l'expiration de votre licence, le programme ne peut plus se

mettre à jour et l'icône d'état de la protection devient rouge.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, cliquez sur **Aide et assistance** pour accéder aux fichiers d'aide ou pour effectuer des recherches dans la base de connaissances ESET. Si vous avez besoin d'aide, vous pouvez envoyer une requête à l'assistance client d'ESET. Le service client ESET répondra très rapidement à vos questions et vous permettra de trouver une solution.

Pour afficher l'**état de la protection**, cliquez sur l'option en haut du menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement d'ESET Mail Security et un sous-menu avec deux options apparaît : **Surveiller l'activité** et **Statistiques**. Sélectionnez l'une de ces options pour afficher des informations détaillées sur votre système.

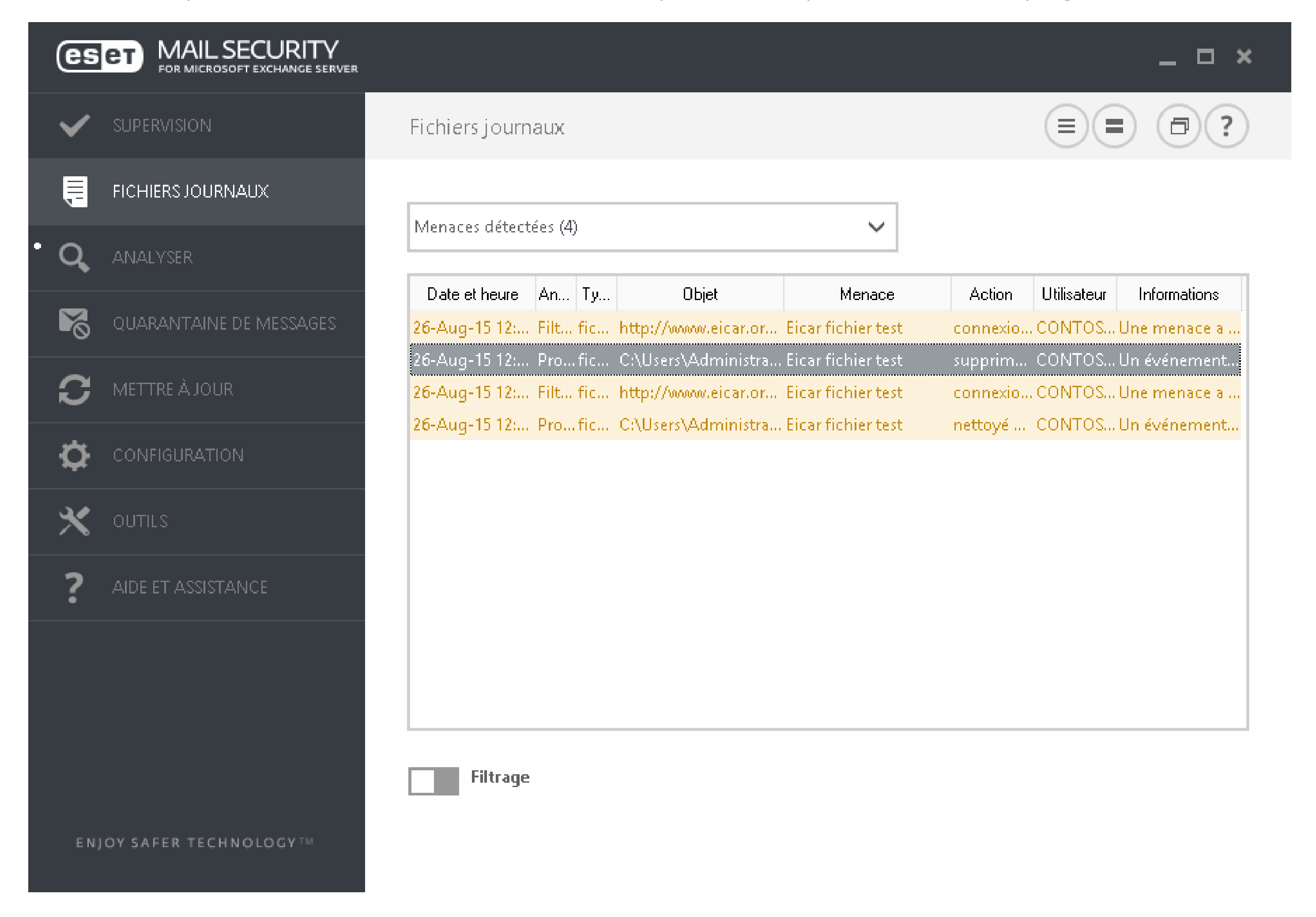
Lorsque ESET Mail Security fonctionne correctement, l'**état de protection** apparaît en vert. Si l'attention est requise, l'icône apparaît en orange ou en rouge.

Cliquez sur **Surveiller l'activité** pour afficher un graphique en temps réel de l'activité du système de fichiers (axe horizontal). L'axe vertical représente les données lues (ligne bleue) et les données écrites (ligne rouge).

Le sous-menu **Statistiques** permet d'afficher le nombre d'objets infectés, nettoyés et propres d'un module défini. Vous pouvez choisir différents modules dans la liste déroulante.

4.2 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. Les journaux sont essentiels pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de détail. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET Mail Security ou de les exporter vers d'autres programmes.



Vous pouvez accéder aux fichiers journaux depuis la fenêtre principale du programme en cliquant sur **Fichiers journaux**. Sélectionnez le type de journal à partir du menu déroulant. Les journaux suivants sont disponibles :

- **Menaces détectées** - Le journal des menaces contient des informations sur les infiltrations détectées par les modules ESET Mail Security. Ces informations comprennent l'heure de détection, le nom de l'infiltration, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où l'infiltration a été détectée. Double-cliquez sur une entrée du journal pour afficher son contenu dans une fenêtre distincte.
- **Événements** - Toutes les actions importantes exécutées par ESET Mail Security sont enregistrées dans le journal des événements. Le journal des événements contient des informations sur les événements qui se sont produits dans le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Ces informations peuvent souvent contribuer à trouver une solution à un problème qui s'est produit dans le programme.
- **Analyse de l'ordinateur** - Tous les résultats des analyses sont affichés dans cette fenêtre. Chaque ligne correspond à un seul contrôle d'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse correspondante.
- **HIPS** - Contient des entrées de règles spécifiques qui sont marquées pour enregistrement. Le protocole affiche l'application qui a appelé l'opération, le résultat (si la règle a été autorisée ou bloquée), ainsi que le nom de la règle créée.
- **Sites Web filtrés** - Liste des sites Web bloqués par la protection de l'accès Web. Ces journaux permettent de voir l'heure, l'URL, l'utilisateur et l'application ayant ouvert une connexion au site Web en question.
- **Contrôle de périphérique** - Contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle de périphérique seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du fournisseur et la taille du support (le cas échéant).
- **Analyse de base de données** - Contient la version de la base des signatures de virus, la date, l'emplacement analysé, le nombre d'objets analysés, le nombre de menaces détectées, le nombre d'applications des règles et l'heure d'achèvement.
- **Protection du serveur de messagerie -** Tous les messages classés par ESET Mail Security comme courrier indésirable ou courrier indésirable probable sont enregistrés ici. Ces journaux s'appliquent aux types de protection suivants : antispam, règles et antivirus.
- **Mise en liste grise** - Tous les messages qui ont été évalués à l'aide de la méthode de mise en liste grises sont enregistrés dans ce journal.

Dans chaque section, vous pouvez copier les informations affichées dans chaque section dans le Presse-papiers (à l'aide du raccourci clavier Ctrl + C) en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**. Pour sélectionner plusieurs entrées, vous pouvez utiliser les touches CTRL et MAJ.

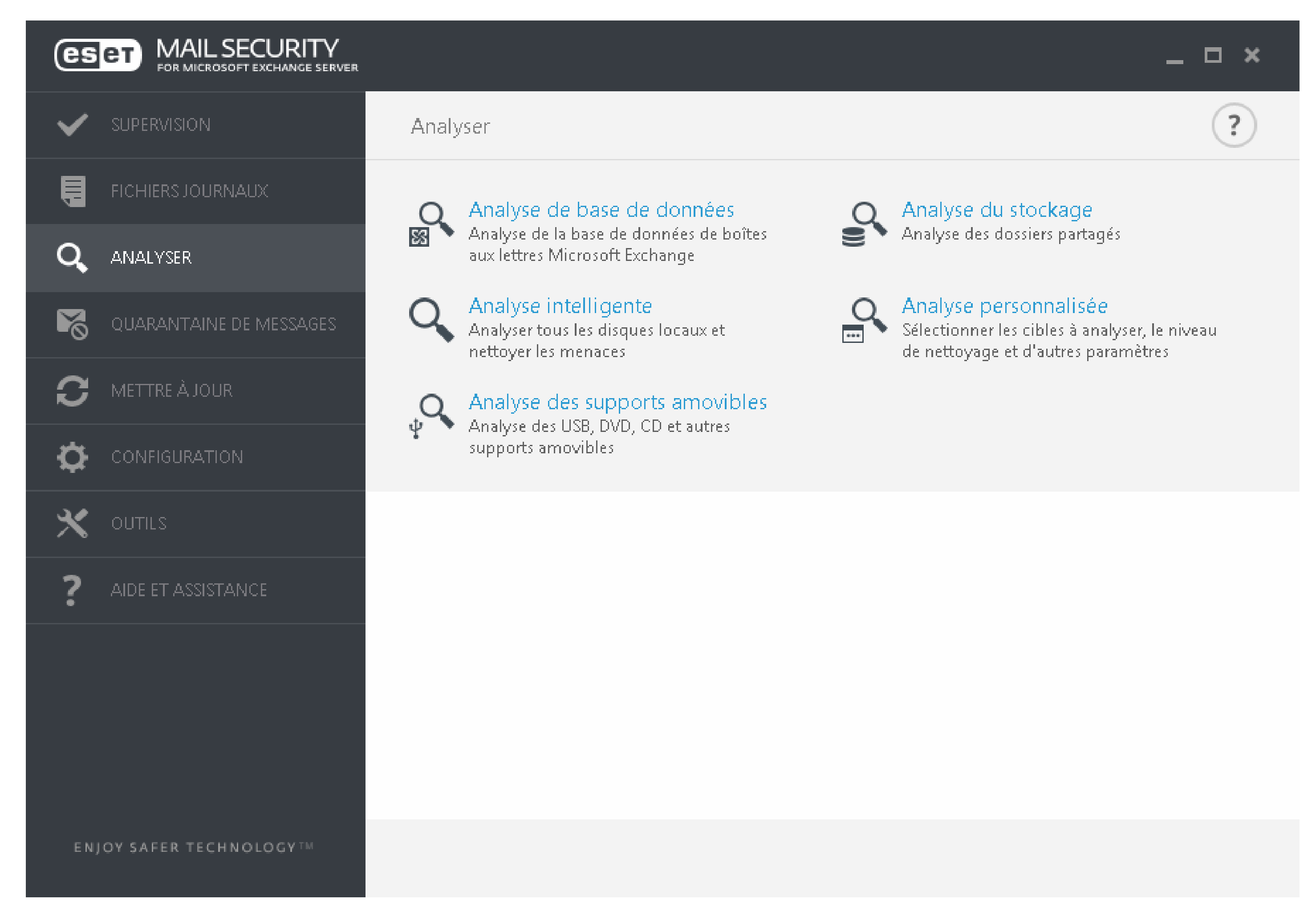
Cliquez sur l'icône de commutateur **Filtrage** pour ouvrir la fenêtre **Filtrage des journaux** dans laquelle vous pouvez définir les critères de filtrage.

Vous pouvez afficher le menu contextuel d'une entrée en cliquant avec le bouton droit sur celle-ci. Le menu contextuel permet d'accéder aux options suivantes :

- **Afficher** - Affiche des détails supplémentaires sur le journal sélectionné dans une nouvelle fenêtre (identique à un double-clic).
- **Filtrer les enregistrements identiques** - Cette option active le filtrage des journaux et affiche uniquement les enregistrements du même type que celui sélectionné.
- **Filtrer...** - Après avoir cliqué sur cette option, la fenêtre Filtrage des journaux permet de définir des critères de filtrage pour des entrées de journal spécifiques.
- **Activer le filtre** - Active les paramètres du filtre. La première fois que vous filtrez les journaux, vous devez définir vos critères de filtrage. Une fois les filtres définis, ils restent identiques jusqu'à leur modification.
- **Copier** - Copie les informations des entrées sélectionnées/en surbrillance dans le Presse-papiers.
- **Copier tout** - Copie les informations de toutes les entrées de la fenêtre.
- **Supprimer** - Supprime les entrées sélectionnées/en surbrillance. Cette action requiert des privilèges d'administrateur.
- **Supprimer tout** - Supprime toutes les entrées de la fenêtre. Cette action requiert des privilèges d'administrateur.
- **Exporter...** - Exporte les informations des entrées sélectionnées/en surbrillance dans un fichier XML.
- **Exporter tout...** - Exporte toutes les informations de la fenêtre dans un fichier XML.
- **Rechercher...** - Ouvre la fenêtre Rechercher dans le journal qui permet de définir des critères de recherche. Fonctionne sur le contenu qui a déjà été filtré pour limiter les résultats.
- **Rechercher suivant** - Recherche l'occurrence suivante d'une recherche précédemment définie (au-dessus).
- **Rechercher précédent** - Recherche l'occurrence précédente d'une recherche précédemment définie (au-dessus).
- **Dérouler le journal** - Laissez cette option activée pour que les anciens journaux défilent automatiquement et pour consulter les journaux actifs dans la fenêtre **Fichiers journaux**.

4.3 Analyser

L'analyseur à la demande est un composant important d'ESET Mail Security. Il permet d'analyser des fichiers et des répertoires de votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Nous vous recommandons d'effectuer des analyses en profondeur de votre système de façon régulière (une fois par mois, par exemple) afin de détectés les virus qui ne l'ont pas été par la protection en temps réel du système de fichiers. Cela peut se produire si la protection en temps réel du système de fichiers est désactivée au moment de l'infection, si la base des signatures de virus n'est plus à jour ou si le fichier n'a pas été détecté comme virus lors de son enregistrement sur le disque.



Deux types d'**analyses de l'ordinateur** sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis et de sélectionner des cibles spécifiques à analyser.

Reportez-vous au chapitre sur la progression de l'analyse pour plus d'informations sur le processus d'analyse.

Analyse du stockage

Analyse tous les dossiers partagés sur le serveur local. Si l'option **Analyse du stockage** n'est pas disponible, cela signifie qu'aucun dossier partagé ne se trouve sur le serveur.

Analyse Hyper-V

Cette option s'affiche dans le menu uniquement si Hyper-V Manager est installé sur le serveur qui exécute ESET Mail Security. L'analyse Hyper-V permet d'analyser les disques d'une machine virtuelle sur un serveur Microsoft Hyper-V sans que le moindre agent ne soit installé sur cette machine virtuelle spécifique. Pour plus d'informations, reportez-vous à la section Analyse Hyper-V.

Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. L'analyse intelligente présente l'intérêt d'être facile à utiliser et de ne pas nécessiter de configuration détaillée. L'analyse intelligente vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage.

Analyse personnalisée

L'analyse personnalisée est une solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. Elle a l'avantage de permettre la configuration précise des paramètres. Les configurations peuvent être enregistrées dans des profils d'analyse définis par l'utilisateur, qui sont utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis sélectionnez une option dans le menu déroulant **Cibles à analyser** ou sélectionnez des cibles spécifiques dans l'arborescence. Une cible à analyser peut également être spécifiée en indiquant le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez effectuer uniquement une analyse du système sans actions de nettoyage supplémentaires, sélectionnez **Analyse sans nettoyage**. Lors d'une analyse, vous pouvez effectuer un choix parmi trois niveaux de nettoyage en cliquant sur **Configuration** > **Paramètres ThreatSense** > **Nettoyage**.

L'exécution d'analyses personnalisées de l'ordinateur n'est recommandée qu'aux utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

Analyse de supports amovibles

Semblable à l'analyse intelligente, ce type d'analyse lance rapidement une analyse des supports amovibles (par ex. CD/DVD/USB) qui sont connectés à l'ordinateur. Cela peut être utile lorsque vous connectez une clé USB à un ordinateur et que vous souhaitez l'analyser pour y rechercher les logiciels malveillants et autres menaces potentielles.

Pour lancer ce type d'analyse, vous pouvez aussi cliquer sur **Analyse personnalisée**, puis sélectionner **Supports amovibles** dans le menu déroulant **Cibles à analyser** et cliquer sur **Analyser**.

Répéter la dernière analyse

Exécute la dernière analyse (analyse du stockage, analyse intelligente, analyse personnalisée, etc.) avec les mêmes paramètres.

i **REMARQUE :** nous recommandons d'exécuter une analyse d'ordinateur au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.

4.3.1 Analyse Hyper-V

L'analyse antivirus Hyper-V permet d'analyser les disques d'un serveur Microsoft Hyper-V, c'est-à-dire d'une machine virtuelle, sans que le moindre agent ne soit installé sur cette machine virtuelle spécifique. L'antivirus est installé en utilisant les privilèges d'administrateur du serveur Hyper-V.

L'analyse Hype-V est issue du module d'analyse de l'ordinateur à la demande, tandis que certaines fonctionnalités n'ont pas été mises en œuvre (analyse du secteur d'amorçage - seront mises en œuvre ultérieurement, comme l'analyse de la mémoire vive.

Systèmes d'exploitation pris en charge

- Windows Server 2008 R2 - Il est possible d'analyser les machines virtuelles fonctionnant sous ce système d'exploitation uniquement lorsqu'elles sont hors ligne
- Windows Server 2012
- Windows Server 2012 R2

Configuration matérielle requise

Le serveur ne doit pas être confronté à des problèmes de performance lorsqu'il exécute des machines virtuelles. L'analyse en elle-même utilise principalement uniquement les ressources du processeur.
En cas d'analyse de machines virtuelles en ligne, il est nécessaire de disposer d'un espace libre sur le disque. L'espace libre sur le disque (pouvant être utilisé) doit être au moins deux fois supérieur à l'espace utilisé par les captures d'écran et les disques virtuels.

La machine virtuelle à analyser est hors ligne (désactivée)

Nous détectons les disques du système d'exploitation de la machine virtuelle à l'aide d'Hyper-V Management et de la prise en charge de disques virtuels et nous nous y connectons. De cette manière, nous accédons de la même manière au contenu des disques que lorsque nous accédons aux fichiers d'un disque dur standard.

La machine virtuelle à analyser est en ligne (en cours d'exécution, en pause, enregistrée)

Nous détectons les disques du système d'exploitation de la machine virtuelle à l'aide d'Hyper-V Management et de la prise en charge de disques virtuels. La connexion générique aux disques n'est pas disponible pour l'instant. Par conséquent, nous créons une capture d'écran de la machine virtuelle et nous l'utilisons pour nous connecter aux disques en mode de lecture seule. La capture d'écran est ensuite supprimée au terme de l'analyse.
La création d'une capture d'écran est une opération lente qui peut prendre de quelques secondes à une minute. Ce détail doit être pris en compte lors de l'application d'une analyse Hyper-V à un nombre de machines virtuelles plus important.

REMARQUE : jusqu'à présent, l'analyse Hyper-V est uniquement une analyse en mode de lecture seule, tant pour une machine virtuelle en ligne que hors ligne. Le nettoyage des infiltrations détectées sera uniquement mise en œuvre ultérieurement.

Nomenclature

Le module de l'analyse Hyper-V doit respecter la nomenclature suivante :
`VirtualMachineName\DiskX\VolumeY`

X représentant le nombre de disques et Y le nombre de volumes.
Par ex. : « `Computer\Disk0\Volume1` ».

Le suffixe du nombre est ajouté en fonction de l'ordre de détection, qui est identique à l'ordre que l'on retrouve dans le Gestionnaire de disques de la machine virtuelle.
Cette nomenclature est utilisée dans la liste arborescente des cibles à analyser, dans la barre de progression et dans les fichiers journaux.

Exécution d'une analyse

Il est possible d'exécuter une analyse de 3 manières :

- À la demande - Si vous cliquez sur l'option Analyse Hyper-V dans le menu de ESET Mail Security, une liste des machines virtuelles disponibles (le cas échéant) à analyser va s'afficher. Il s'agit d'une liste arborescente dans laquelle l'entité du niveau le plus bas est un volume, ce qui signifie qu'il n'est pas possible de sélectionner un répertoire ou un fichier à analyser, étant donné que l'intégralité du volume doit être analysée.
  Afin de dresser la liste des volumes disponibles, nous devons nous connecter au(x) disque(s) virtuels (s) particulier(s), ce qui peut prendre quelques secondes. Par conséquent, une action plus rapide consiste à marquer la machine virtuelle ou son/ses disques(s) à analyser.
  Dès que vous avez marqué les machines virtuelles, les disques ou les volumes à analyser, cliquez sur le bouton Analyser.
- Via le planificateur
- Via ERA en tant que tâche de client appelée Analyse du serveur. L'entité du niveau le plus bas à analyser est un disque d'une machine virtuelle.

Il est possible d'exécuter simultanément plusieurs analyses Hyper-V.

Une notification vous avertira de la fin de l'analyse et vous pourrez prendre connaissance des détails d'une analyse réalisée en suivant un lien Afficher les fichiers journaux. Tous les journaux d'analyse sont disponibles dans la section Fichiers journaux de ESET Mail Security, mais vous devez sélectionner l'analyse Hyper-V dans le menu déroulant afin d'afficher les journaux associés.

Problèmes éventuels

- Lors de l'exécution de l'analyse d'une machine virtuelle en ligne, une capture d'écran de cette machine virtuelle doit être créée. Par ailleurs, au cours de la création d'une capture d'écran, il se peut que certaines actions génériques de la machine virtuelle soient limitées ou désactivées.
- Dans le cas où une machine virtuelle est analysée, elle ne peut pas être activée avant la fin de l'analyse.
- Hyper-V Manager vous permet de donner un nom identique à deux machines virtuelles, ce qui peut s'avérer problématique pour différentier les machines pendant la consultation des journaux d'analyse.

4.4 Quarantaine de messages

Le gestionnaire de quarantaine de messages est disponible pour les trois types de quarantaine :

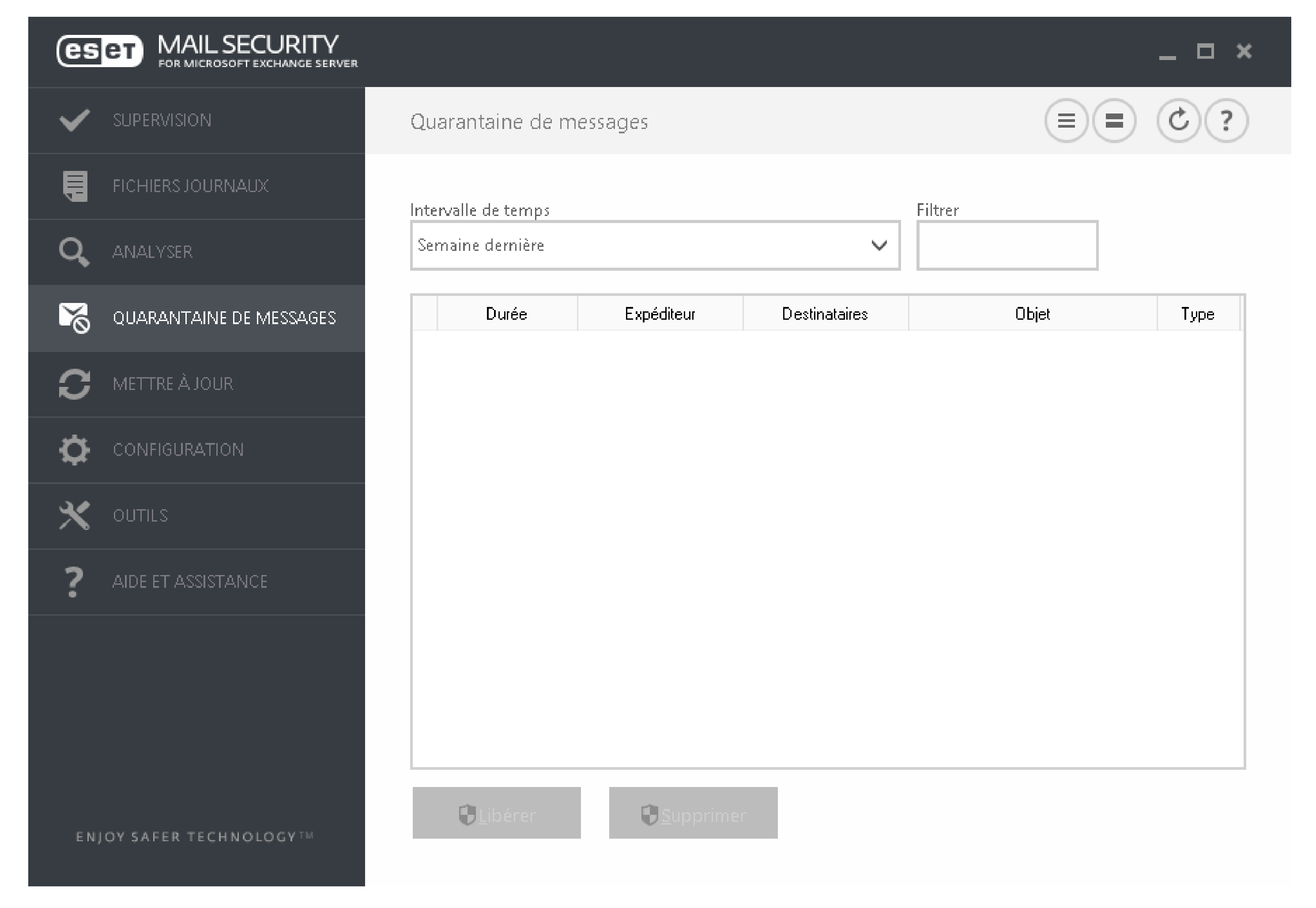
- Quarantaine locale
- Boîte aux lettres de quarantaine
- Quarantaine MS Exchange

REMARQUE : l'interface Web Quarantaine de messages est une solution que vous pouvez utiliser à la place du gestionnaire de quarantaine de messages pour gérer les objets de message électronique mis en quarantaine.

Filtrage

- **Intervalle de temps** : vous pouvez sélectionner l'intervalle de temps pendant lequel les messages électroniques sont affichés (1 semaine par défaut). Lorsque vous modifiez l'intervalle de temps, les éléments de quarantaine de messages sont automatiquement rechargés.
- **Filtrer** : vous pouvez utiliser la zone de texte de filtrage pour filtrer les messages électroniques affichés (toutes les colonnes font l'objet d'une recherche).

REMARQUE : les données du gestionnaire de quarantaine de messages ne sont pas automatiquement mises à jour. Il est recommandé de cliquer régulièrement sur l'icône d'actualisation pour afficher les éléments les plus récents dans la quarantaine de messages.

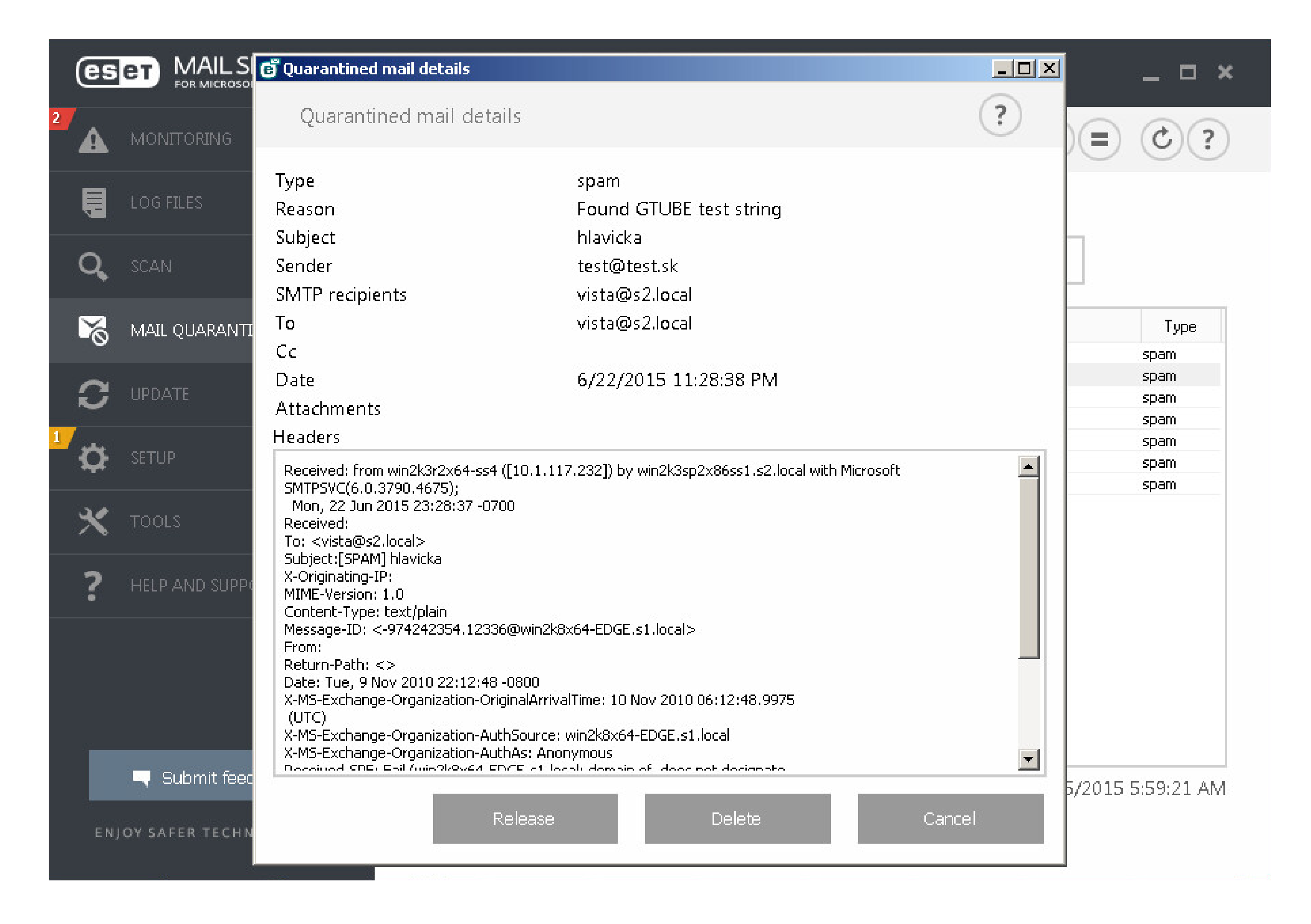


Action

- **Libérer** : libère le message électronique pour le ou les destinataires d'origine à l'aide du répertoire de lecture et le supprime de la quarantaine. Cliquez sur **Oui** pour confirmer l'action.
- **Supprimer** : supprime l'élément de la quarantaine. Cliquez sur **Oui** pour confirmer l'action.

Détails du message mis en quarantaine : double-cliquez sur le message mis en quarantaine ou cliquez avec le bouton droit et sélectionnez **Détails**. Une fenêtre indépendante s'ouvre alors. Elle contient des détails sur le message électronique mis en quarantaine. Des informations supplémentaires sur le courrier électronique figurent également dans l'en-tête de courrier électronique RFC.

Ces actions sont également disponibles dans le menu contextuel. Si vous le souhaitez, cliquez sur **Libérer**, **Supprimer** ou **Supprimer définitivement** pour exécuter une action sur un message électronique mis en quarantaine. Cliquez sur **Oui** pour confirmer l'action. Si vous choisissez **Supprimer définitivement**, le message est également supprimé du système de fichiers, contrairement à l'option **Supprimer** qui supprime l'élément de la vue du gestionnaire de quarantaine de messages.



4.4.1 Détails du message électronique mis en quarantaine

Cette fenêtre contient les informations suivantes sur le message électronique : **Type**, **Motif**, **Objet**, **Expéditeur**, **Destinataires SMTP**, **À**, **Cc**, **Date**, **Pièces jointes** et **En-têtes**. Vous pouvez sélectionner les en-têtes, les copier et les coller en cas de besoin.

Vous pouvez exécuter une action sur le message électronique mis en quarantaine à l'aide des boutons suivants :

- **Libérer** : libère le message électronique pour le ou les destinataires d'origine à l'aide du répertoire de lecture et le supprime de la quarantaine. Cliquez sur **Oui** pour confirmer l'action.
- **Supprimer** : supprime l'élément de la quarantaine. Cliquez sur **Oui** pour confirmer l'action.

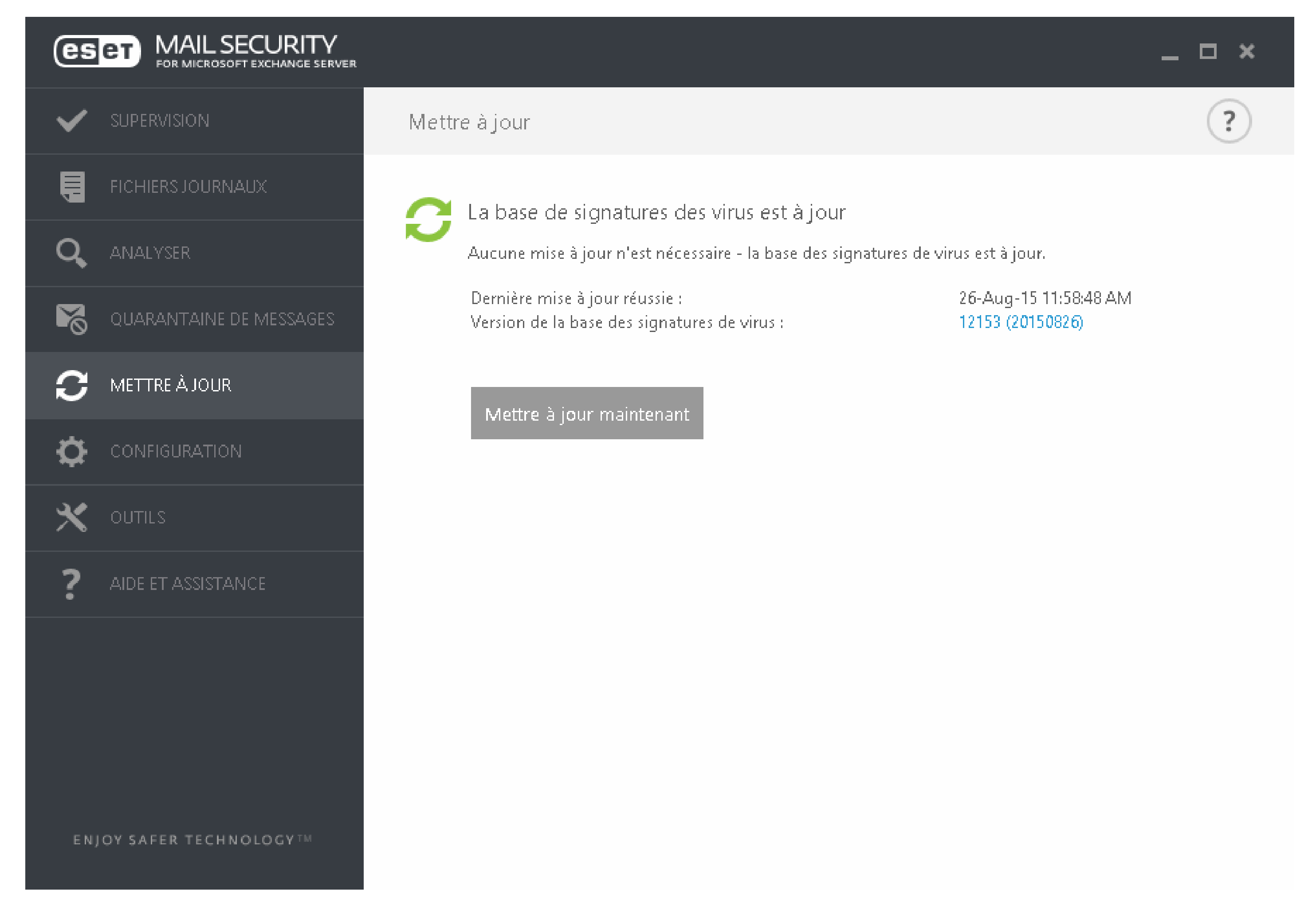
Cliquez sur le bouton **Annuler** pour fermer la fenêtre Détails du message électronique mis en quarantaine.

4.5 Mise à jour

La mise à jour régulière d'ESET Mail Security est la meilleure méthode pour conserver le niveau maximum de sécurité de votre ordinateur. Le module de mise à jour veille à ce que le programme soit toujours à jour de deux façons : en mettant à jour la base des signatures de virus et en mettant à jour les composants système.

En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

Pour commencer le processus de mise à jour, cliquez sur **Mettre à jour maintenant**. La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes de la protection totale contre les attaques des codes malveillants.



Dernière mise à jour réussie - Date de la dernière mise à jour. Vérifiez qu'il s'agit d'une date récente indiquant que la base des signatures de virus est à jour.

Version de la base des signatures de virus : numéro de la base des signatures de virus ; il s'agit également d'un lien actif vers le site Web d'ESET. Cliquez ici pour afficher la liste de toutes les signatures ajoutées dans une mise à jour.

Processus de mise à jour

Lorsque vous avez cliqué sur **Mettre à jour maintenant**, le processus de téléchargement commence et la progression de la mise à jour s'affiche. Pour interrompre la mise à jour, cliquez sur **Annuler la mise à jour**.

Important : dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **Mise à jour non nécessaire - la base des signatures de virus installée est à jour** s'affiche dans la fenêtre **Mise à jour**. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veillez à mettre à jour la base des signatures de virus dès que possible. Dans d'autres circonstances, l'un des messages d'erreur suivants s'affiche :

La base des signatures de virus n'est plus à jour - Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour de la base des signatures de virus. Nous vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de données d'authentification ou de la configuration incorrecte des paramètres de connexion.

La notification précédente concerne les deux messages **Échec de la mise à jour de la base des signatures de virus** sur les mises à jour infructueuses :

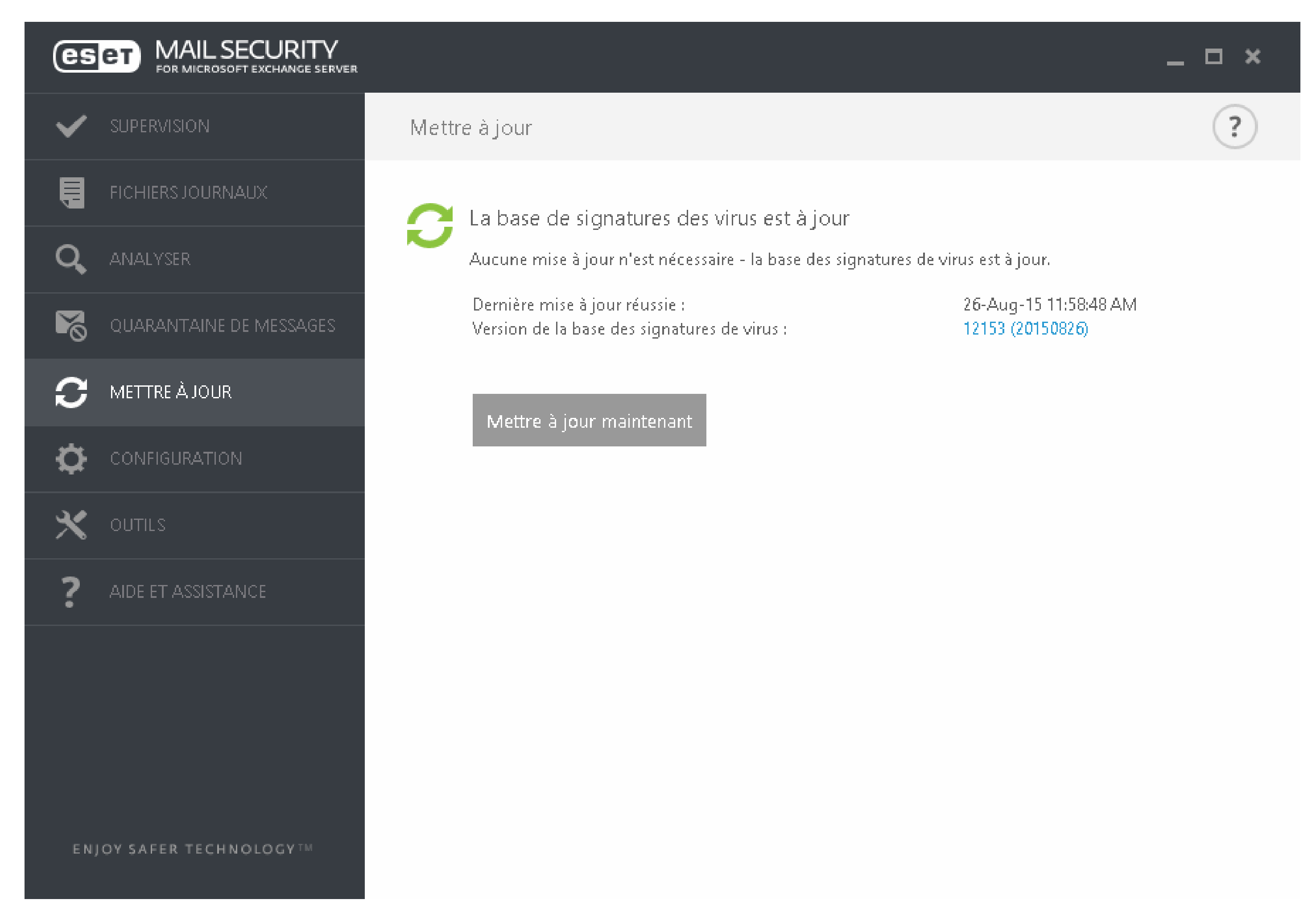
Licence non valide - La clé de licence n'a pas été correctement saisie lors de la configuration des mises à jour. Nous vous recommandons de vérifier vos données d'authentification. La fenêtre Configuration avancée (appuyez sur la touche F5 de votre clavier) contient d'autres options de mise à jour. Dans le menu principal, cliquez sur **Aide et assistance** > **Gérer la licence** pour saisir une nouvelle clé de licence.

Une erreur s'est produite pendant le téléchargement des fichiers de mise à jour - Cette erreur peut être due à des paramètres de connexion Internet incorrects. Nous vous recommandons de vérifier votre connectivité à Internet en ouvrant un site Web dans votre navigateur. Si le site Web ne s'ouvre pas, cela est probablement dû au fait qu'aucune connexion à Internet n'est établie ou que votre ordinateur a des problèmes de connectivité. Consultez votre fournisseur de services Internet si vous n'avez pas de connexion Internet active.

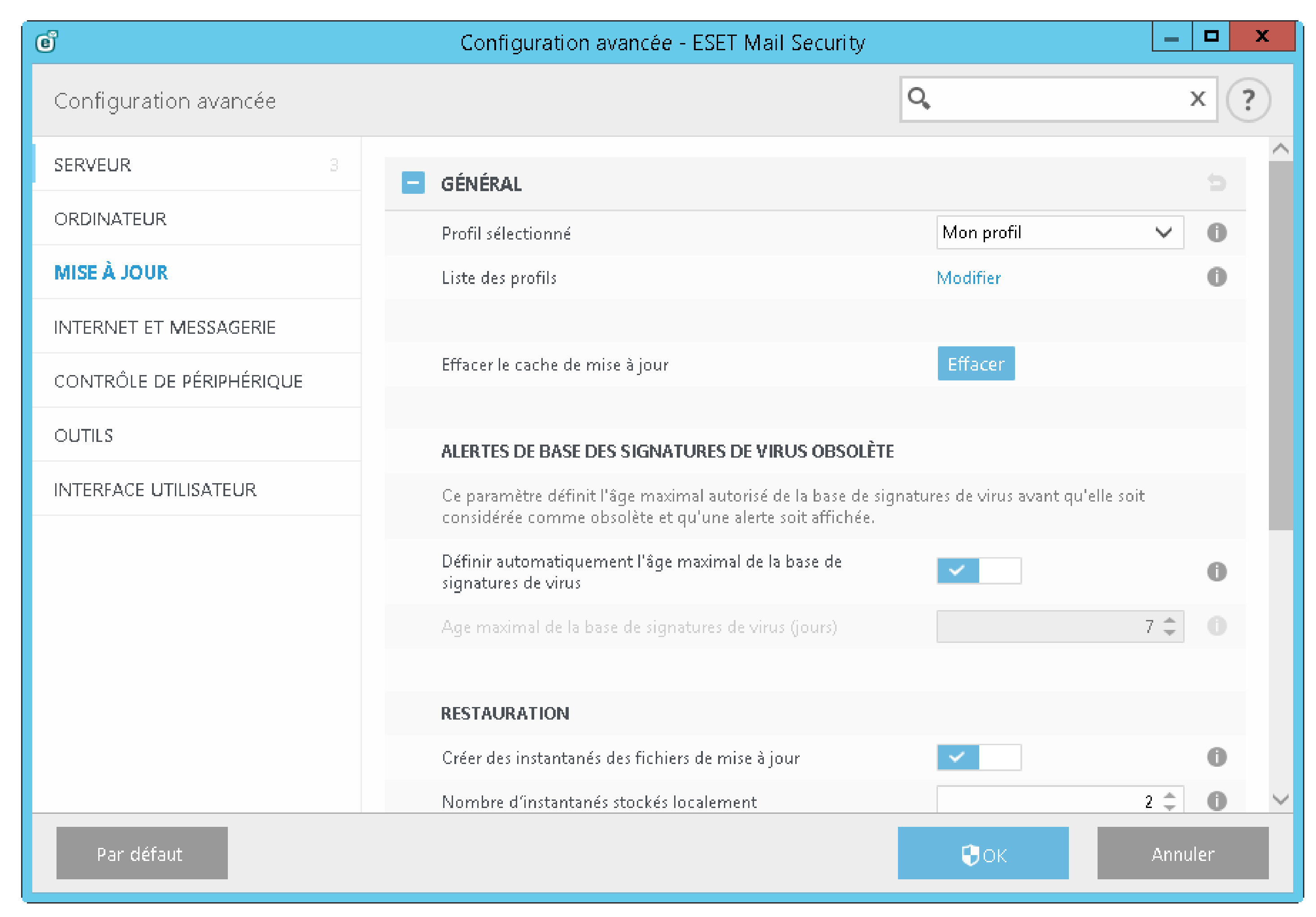
i **REMARQUE :** pour plus d'informations, consultez cet article de la base de connaissances ESET.

4.5.1 Configuration de la mise à jour de la base des virus

La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes qui assurent la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à leur configuration et à leur fonctionnement. Dans le menu principal, accédez à **Mettre à jour**, puis cliquez sur **Mettre à jour maintenant** pour rechercher toute nouvelle base des signatures.



Vous pouvez configurer les paramètres de mise à jour dans la fenêtre Configuration avancée (appuyez sur la touche F5 du clavier). Pour configurer les options avancées de mise à jour telles que le mode de mise à jour, l'accès au serveur proxy, la connexion LAN et les paramètres de copie de signature de virus (miroir), cliquez sur **Mettre à jour** dans la fenêtre **Configuration avancée** située à gauche. En cas de problème de mise à jour, cliquez sur **Effacer le cache** pour effacer le dossier de mise à jour temporaire. Le menu **Serveur de mise à jour** est défini par défaut sur **SÉLECTION AUTOMATIQUE**. L'option **SÉLECTION AUTOMATIQUE** signifie que le serveur de mise à jour à partir duquel les mises à jour des signatures de virus sont téléchargées est sélectionné automatiquement. Il est recommandé de conserver cette option par défaut. Si vous ne souhaitez pas afficher les notifications de la barre d'état système dans l'angle inférieur droit de l'écran, sélectionnez **Désactiver l'affichage d'une notification de réussite de la mise à jour**.

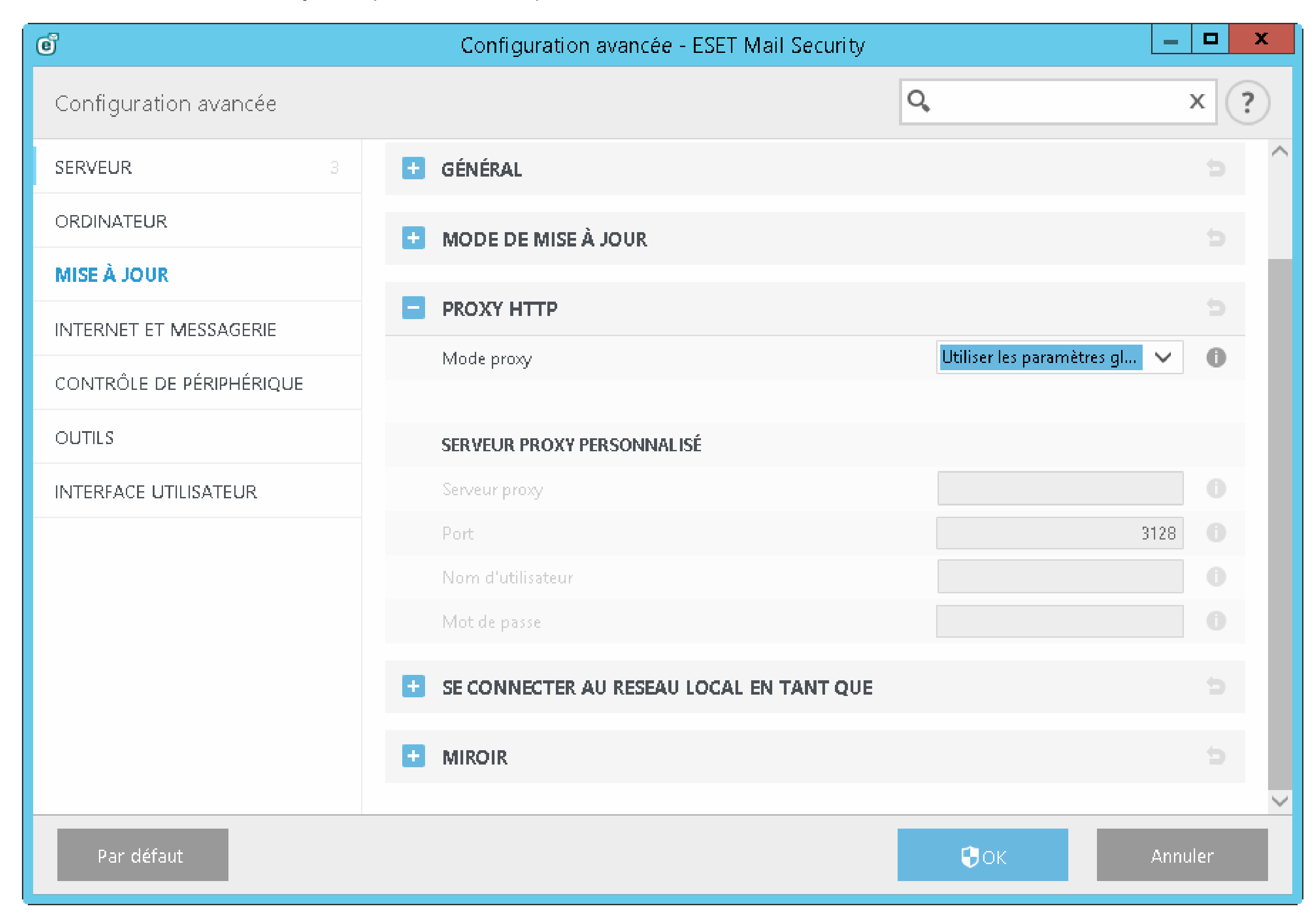


Le programme doit être mis à jour automatiquement pour assurer un fonctionnement optimal. Cela n'est possible que si la **clé de licence** correcte est entrée dans **Aide et assistance** > **Activer la licence.**

Si vous n'avez pas activé votre produit après l'installation, vous pouvez le faire à tout moment. Pour plus d'informations sur l'activation, reportez-vous à la section Comment activer ESET Mail Security, puis entrez les données de licence que vous avez reçues avec votre produit de sécurité ESET dans la fenêtre Détails de la licence.

4.5.2 Configuration du serveur proxy pour les mises à jour

Si vous utilisez un serveur proxy pour la connexion Internet sur un système sur lequel ESET Mail Security est installé, les paramètres de proxy doivent être configurés dans Configuration avancée. Pour accéder à la fenêtre de configuration du serveur proxy, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Mettre à jour** > **Proxy HTTP**. Sélectionnez **Connexion via un serveur proxy** dans le menu déroulant **Mode proxy** et indiquez les détails concernant le serveur proxy : l'adresse IP du **serveur proxy**, le numéro de **port**, ainsi que le **nom d'utilisateur** et le **mot de passe** (le cas échéant).



Si vous ne connaissez pas les détails du serveur proxy, vous pouvez essayer de détecter automatiquement les paramètres de ce serveur en sélectionnant **Utiliser les paramètres globaux de serveur proxy** dans la liste déroulante.

i **REMARQUE :** Les options du serveur proxy peuvent varier selon les profils de mise à jour. Si c'est le cas, configurez les différents profils de mise à jour dans Configuration avancée en cliquant sur **Mettre à jour** > **Profil**.

4.6 Configuration

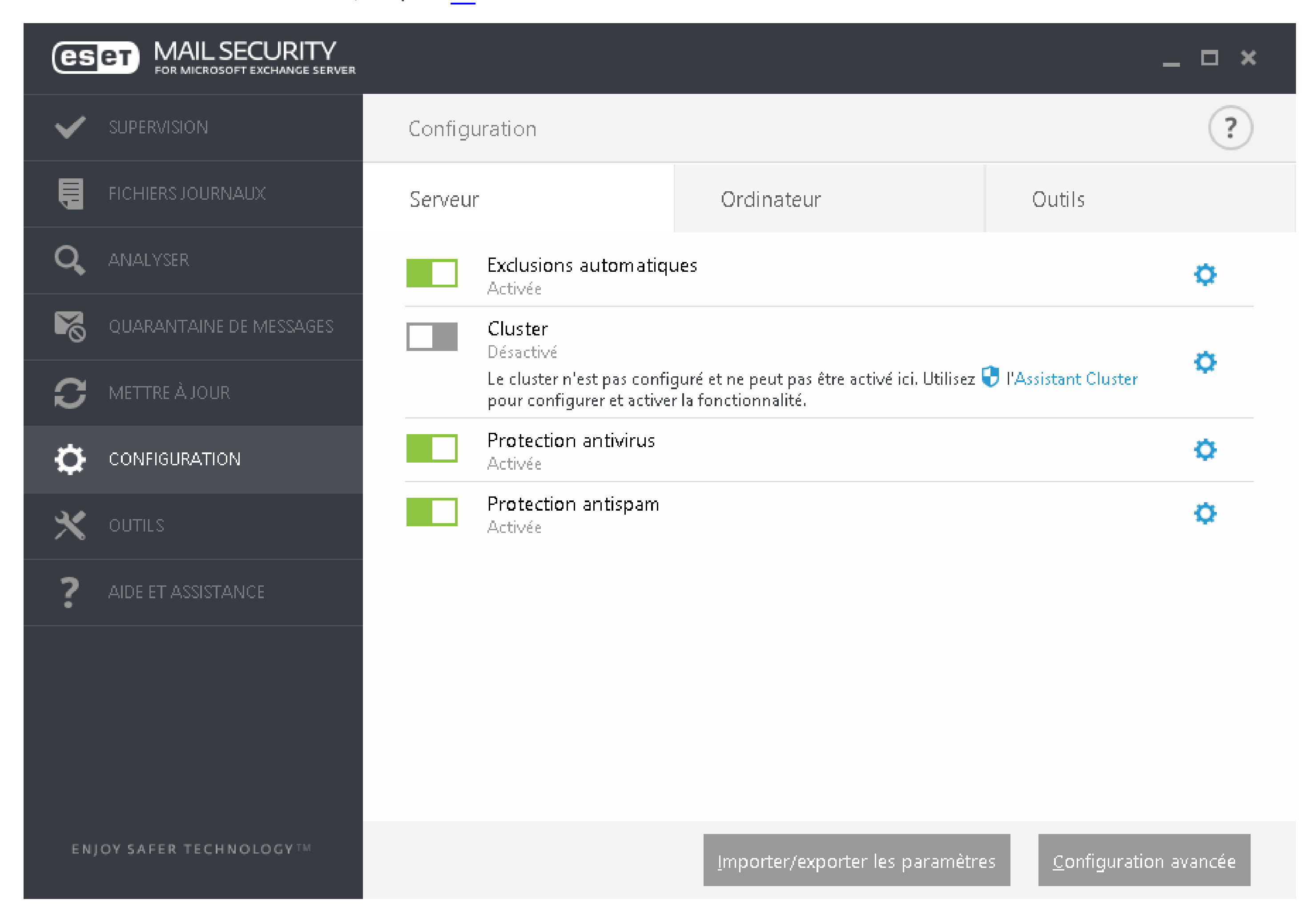
Le menu de configuration est composé de trois onglets :

- Serveur
- Ordinateur
- Outils

4.6.1 Serveur

ESET Mail Security protège votre serveur grâce aux fonctionnalités essentielles suivantes : Antivirus et Antispyware, bouclier résident (protection en temps réel), protection de l'accès Web et protection du client de messagerie. Vous trouverez des informations sur chaque type de protection dans ESET Mail Security - Protection de l'ordinateur.

- Exclusions automatiques - Cette fonctionnalité identifie les applications serveur et les fichiers du système d'exploitation serveur critiques, puis les ajoute automatiquement à la liste des exclusions. Cette fonctionnalité réduira le risque de conflits potentiels et augmentera les performances globales du serveur lors de l'exécution du logiciel antivirus.
- Pour configurer ESET Cluster, cliquez sur **Assistant Cluster**. Pour plus d'informations sur la configuration d'ESET Cluster à l'aide de l'assistant, cliquez ici.



Si vous souhaitez définir des options plus détaillées, cliquez sur **Configuration avancée** ou appuyez sur **F5**.

D'autres options sont disponibles au bas de la fenêtre de configuration. Pour charger les paramètres de configuration à l'aide d'un fichier de configuration *.xml* ou pour enregistrer les paramètres de configuration actuels dans un fichier de configuration, utilisez l'option **Importer/exporter les paramètres**. Pour plus d'informations, consultez la section Importer/exporter les paramètres.

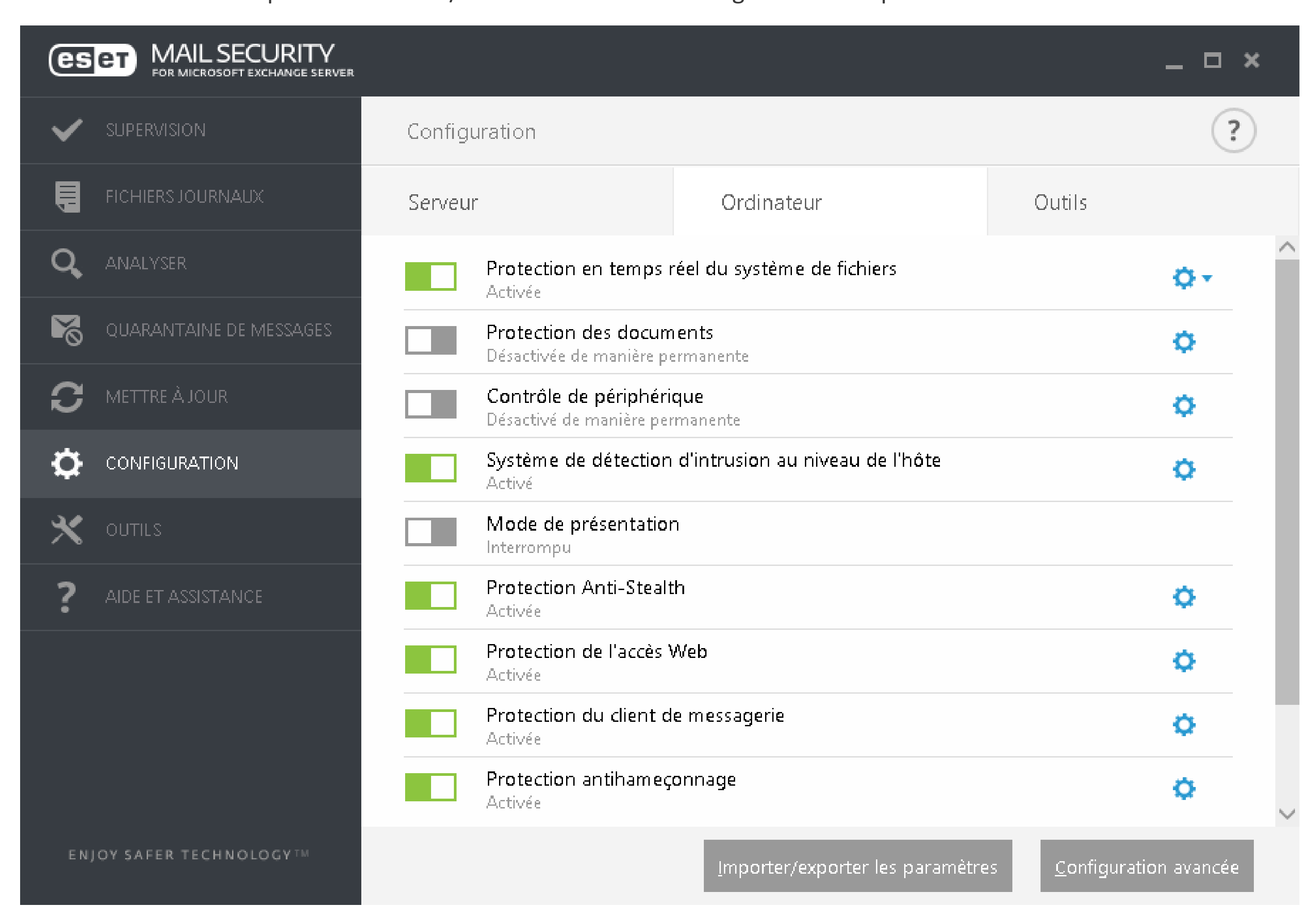
4.6.2 Ordinateur

ESET Mail Security dispose de tous les composants nécessaires pour garantir la protection du serveur en tant qu'ordinateur. Chaque composant fournir un type spécifique de protection : Antivirus et Antispyware, protection du système en temps réel, protection de l'accès Web, protection du client de messagerie, protection anti-hameçonnage, etc.

La section **Ordinateur** est disponible dans **Configuration** > **Ordinateur**. La liste des composants que vous pouvez activer/désactiver à l'aide du bouton s'affiche. Pour configurer les paramètres d'un élément spécifique, cliquez sur l'engrenage . Pour la **protection en temps réel du système de fichiers**, vous pouvez également **modifier les exclusions**. Cette option ouvre la fenêtre de configuration des exclusions dans laquelle vous pouvez exclure de l'analyse des fichiers et des dossiers.

Désactiver la protection antivirus et antispyware - Lorsque vous désactivez temporairement la protection antivirus et antispyware, vous pouvez sélectionner la durée de désactivation du composant sélectionné dans le menu déroulant et cliquer sur **Appliquer** pour désactiver le composant de sécurité. Pour réactiver la protection, cliquez sur **Activer la protection antivirus et antispyware**.

Le module **Ordinateur** permet d'activer/de désactiver et de configurer les composants suivants :



- **Protection en temps réel du système de fichiers** - Tous les fichiers ouverts, créés ou exécutés sur l'ordinateur sont analysés pour y rechercher la présence éventuelle de code malveillant.
- **Protection des documents** - La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que les éléments Microsoft ActiveX.
- **Contrôle de périphérique -** Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/ autorisations, et de définir les autorisations des utilisateurs à accéder à un périphérique et à l'utiliser.
- **HIPS** - Le système HIPS surveille les événements qui se produisent dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.
- **Mode de présentation** - Fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Vous recevez un message d'avertissement (risque potentiel de sécurité) et la fenêtre principale devient orange lorsque le mode de présentation est activé.
- **Protection Anti-Stealth** - Détecte les programmes dangereux tels que les rootkits, qui sont en mesure de se dissimuler du système d'exploitation. Il est impossible de les détecter à l'aide de techniques de test ordinaires.
- **Protection de l'accès Web** - Si cette option est activée, tout le trafic HTTP ou HTTPS est analysé afin d'y rechercher des codes malveillants.
- **Protection du client de messagerie** - Contrôle les communications reçues via les protocoles POP3 et IMAP.
- **Protection antihameçonnage** - Vous protège des tentatives d'acquisition de mots de passe, de données bancaires ou d'autres informations sensibles par des sites Web non légitimes se faisant passer pour des sites Web dignes de confiance.

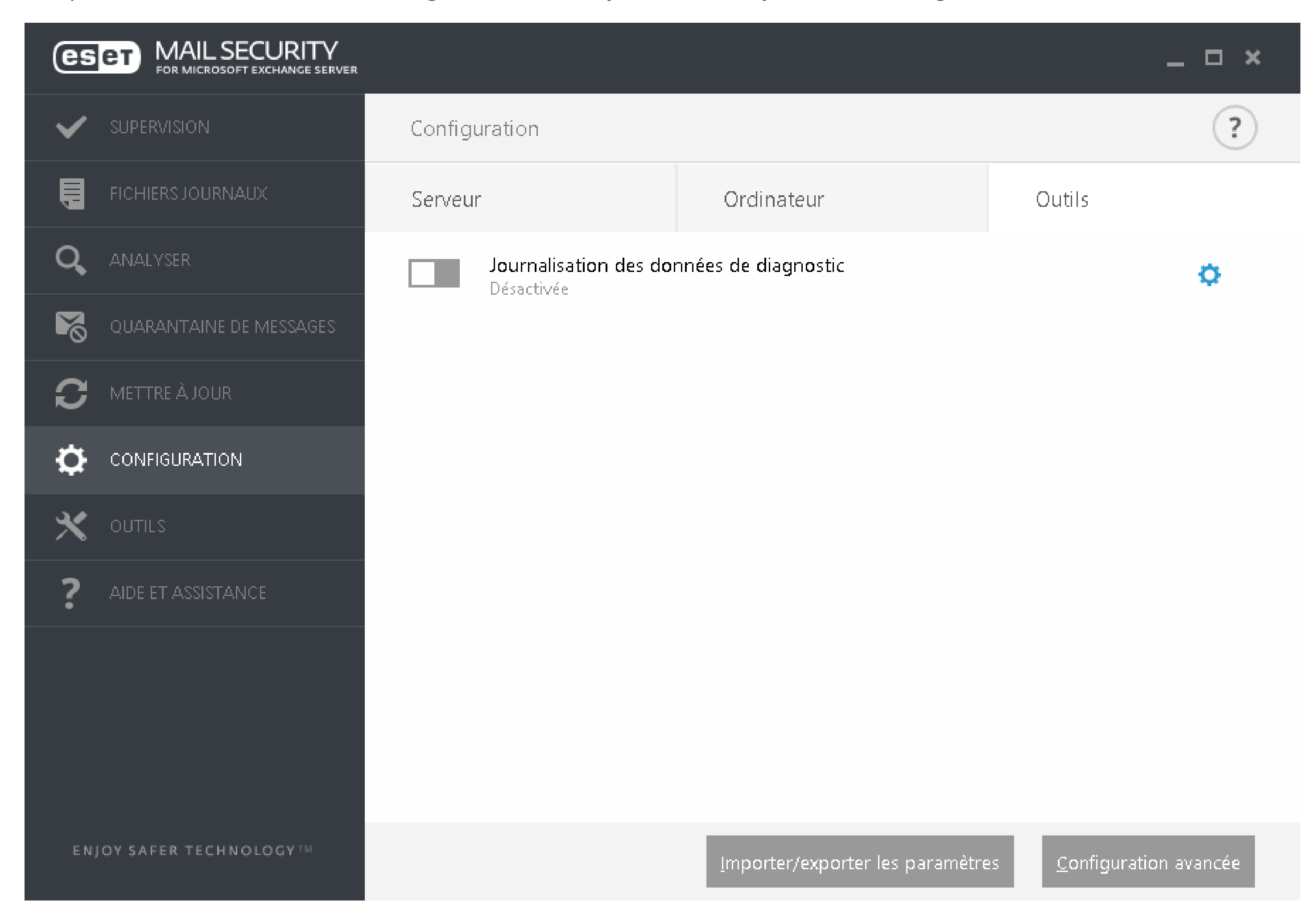
i **REMARQUE :** la protection des documents est désactivée par défaut. Vous pouvez facilement l'activer en cliquant sur l'icône de commutateur.

D'autres options sont disponibles au bas de la fenêtre de configuration. Pour charger les paramètres de configuration à l'aide d'un fichier de configuration *.xml* ou pour enregistrer les paramètres de configuration actuels dans un fichier de configuration, utilisez l'option **Importer/exporter les paramètres**. Pour plus d'informations, consultez la section Importer/exporter les paramètres.

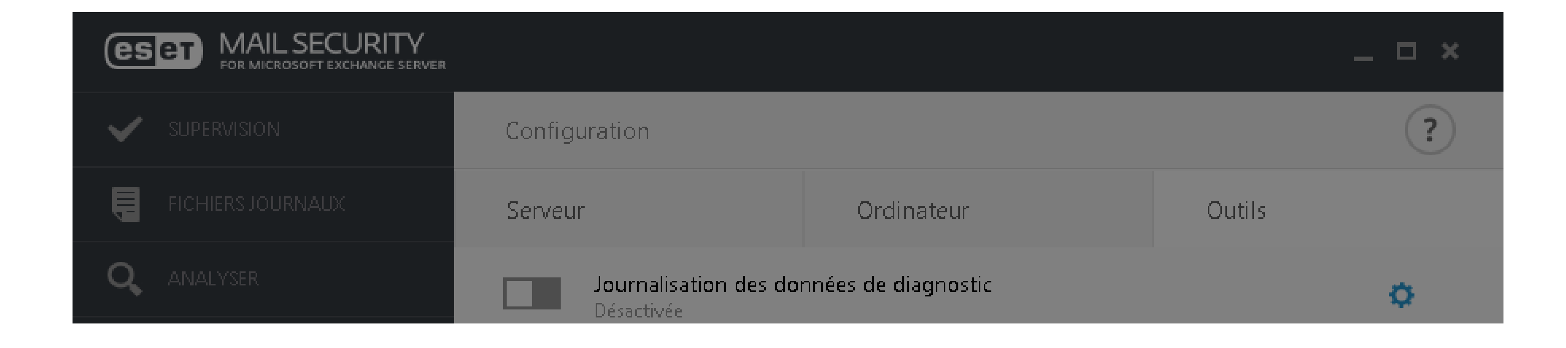
Si vous souhaitez définir des options plus détaillées, cliquez sur **Configuration avancée** ou appuyez sur **F5**.

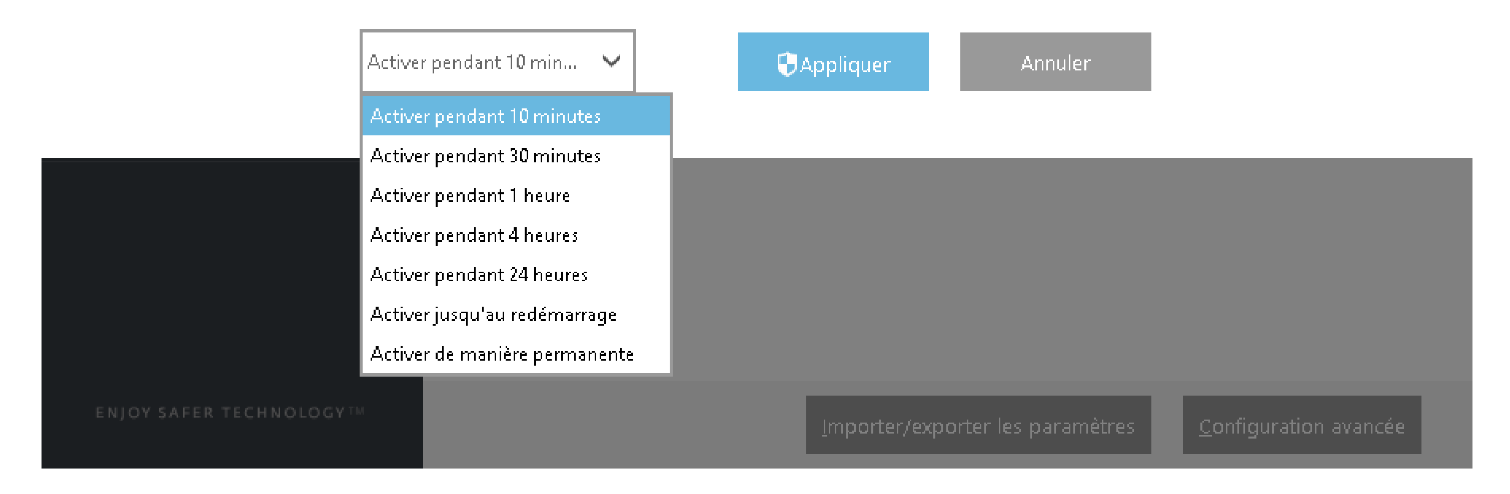
4.6.3 Outils

Journalisation des données de diagnostic : configurez les composants qui écrivent dans les journaux de diagnostic lorsque la journalisation des données de diagnostic est activée. Lorsque vous cliquez sur le bouton bascule pour activer la journalisation des données de diagnostic, vous pouvez choisir la durée de l'activation (10 minutes, 30 minutes, 1 heure, 4 heures, 24 heures, jusqu'au redémarrage suivant du serveur ou de manière permanente). Les composants non affichés dans cet onglet écrivent toujours dans les journaux de diagnostic.



- **Activez** la journalisation des données de diagnostic pendant la période définie.

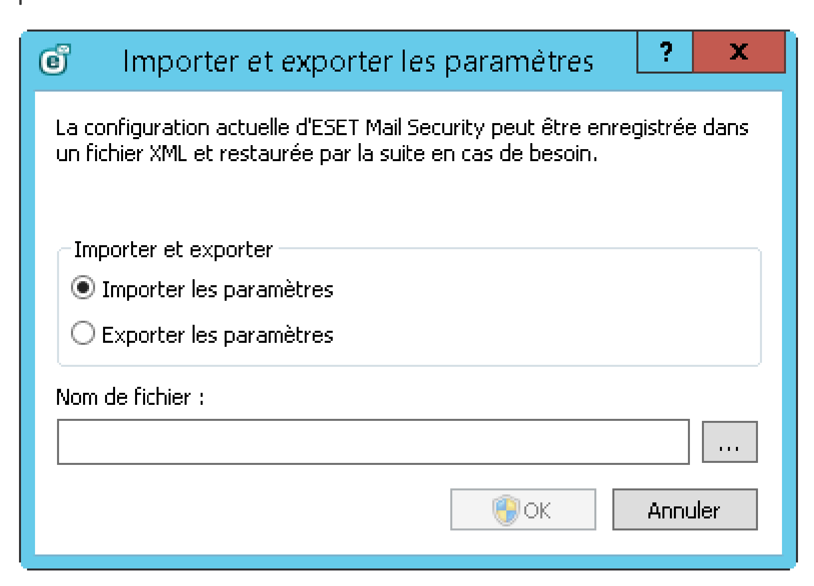




4.6.4 Importer et exporter les paramètres

L'importation et l'exportation de la configuration d'ESET Mail Security sont accessibles dans **Configuration** en cliquant sur **Importer/Exporter les paramètres**.

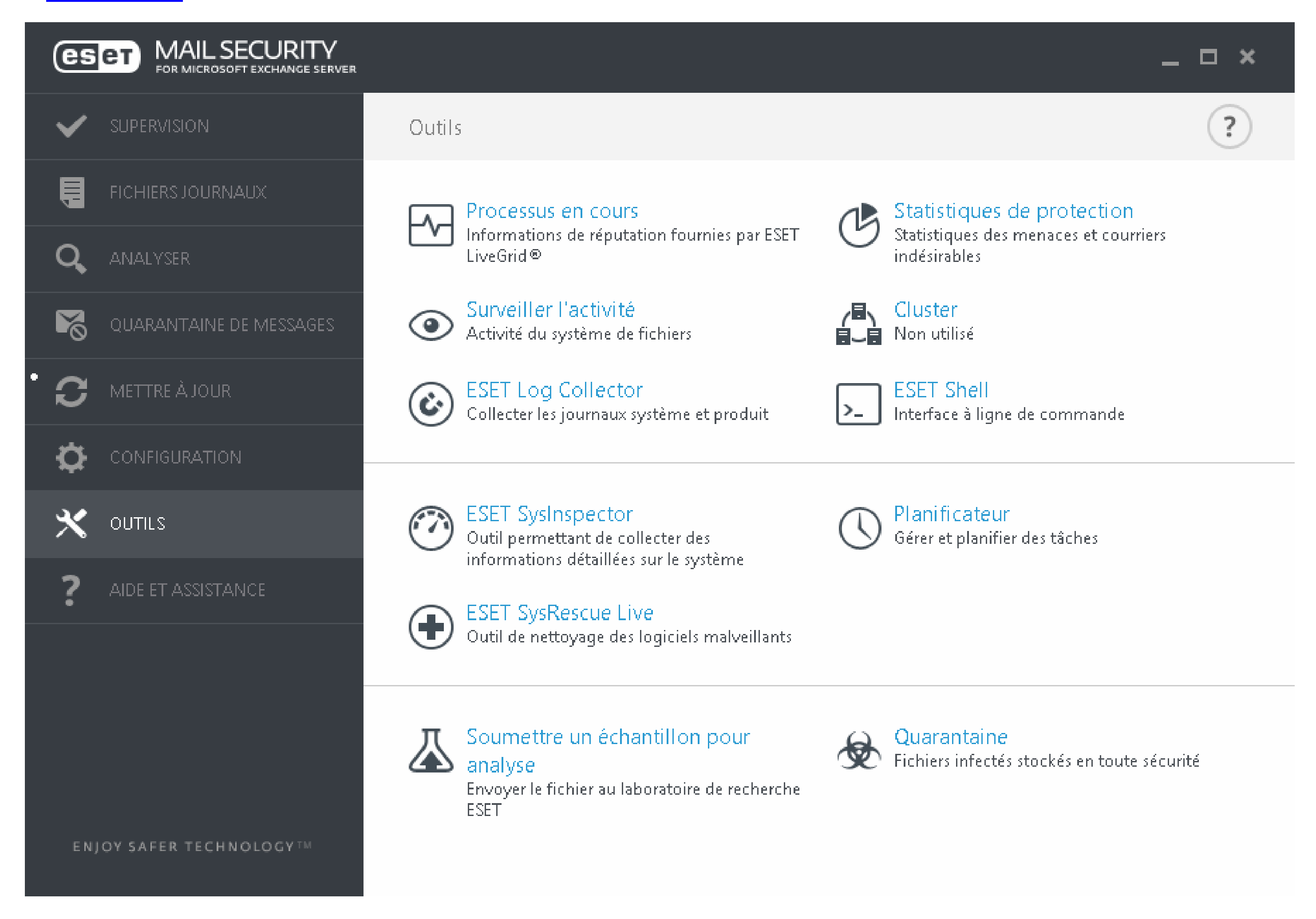
L'importation et l'exportation utilisent le type de fichier .xml. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle d'ESET Mail Security. Elle peut être utilisée ultérieurement pour appliquer les mêmes paramètres à d'autres ordinateurs.



4.7 Outils

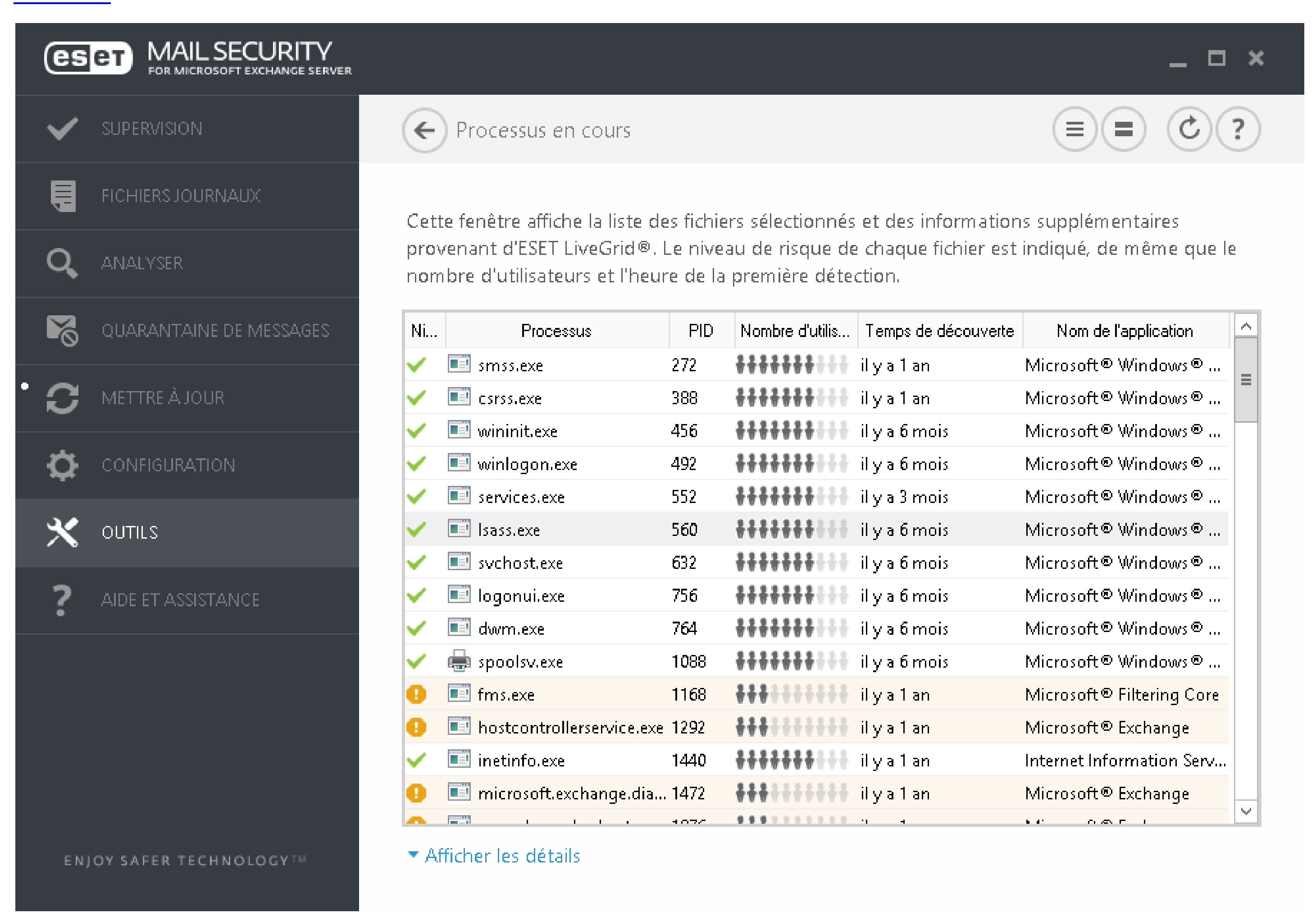
Le menu Outils comprend des modules qui contribuent à simplifier l'administration du programme et offrent des options supplémentaires. Il contient les outils suivants :

- Processus en cours
- Surveiller l'activité
- ESET Log Collector
- Statistiques de protection
- Cluster
- Shell ESET
- ESET SysInspector
- ESET SysRescue Live
- Planificateur
- Soumettre un échantillon pour analyse
- Quarantaine



4.7.1 Processus en cours

Les processus en cours affichent les programmes ou processus en cours d'exécution sur votre ordinateur et informe ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. ESET Mail Security fournit des informations détaillées sur l'exécution des processus afin de protéger les utilisateurs à l'aide de la technologie ESET Live Grid.



Niveau de risque - Dans la majorité des cas, ESET Mail Security et la technologie ESET Live Grid attribuent des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 - OK (vert) à 9 - Risqué (rouge).

Processus - Nom de l'image du programme ou du processus en cours d'exécution sur l'ordinateur. Vous pouvez également utiliser le Gestionnaire de tâches pour afficher tous les processus en cours d'exécution sur votre ordinateur. Vous pouvez ouvrir le Gestionnaire de tâches en cliquant avec le bouton droit de la souris sur une zone vide de la barre des tâches, puis en cliquant sur Gestionnaire de tâches ou en appuyant sur les touches **Ctrl+Maj +Échap** du clavier.

PID - ID des processus en cours d'exécution dans les systèmes d'exploitation Windows.

i **REMARQUE :** les applications connues marquées OK (vert) sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse, ce qui améliore la vitesse de l'analyse d'ordinateur à la demande ou de la protection du système en temps réel sur votre ordinateur.

Nombre d'utilisateurs - Nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET Live Grid.

Temps de découverte - Durée écoulée depuis la détection de l'application par la technologie ESET Live Grid.

i **REMARQUE :**une application marquée avec le niveau de sécurité Inconnu (orange) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Vous pouvez soumettre un échantillon pour

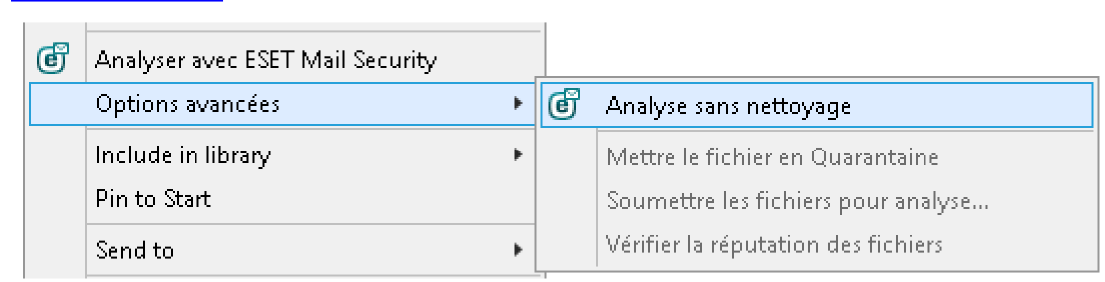
analyse au laboratoire ESET si ce fichier vous semble suspect. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à l'une des prochaines mises à jour de la base des signatures de virus.

Nom de l'application - Nom attribué à un programme auquel appartient ce processus.

Lorsque vous cliquez sur une application située au bas de la fenêtre, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

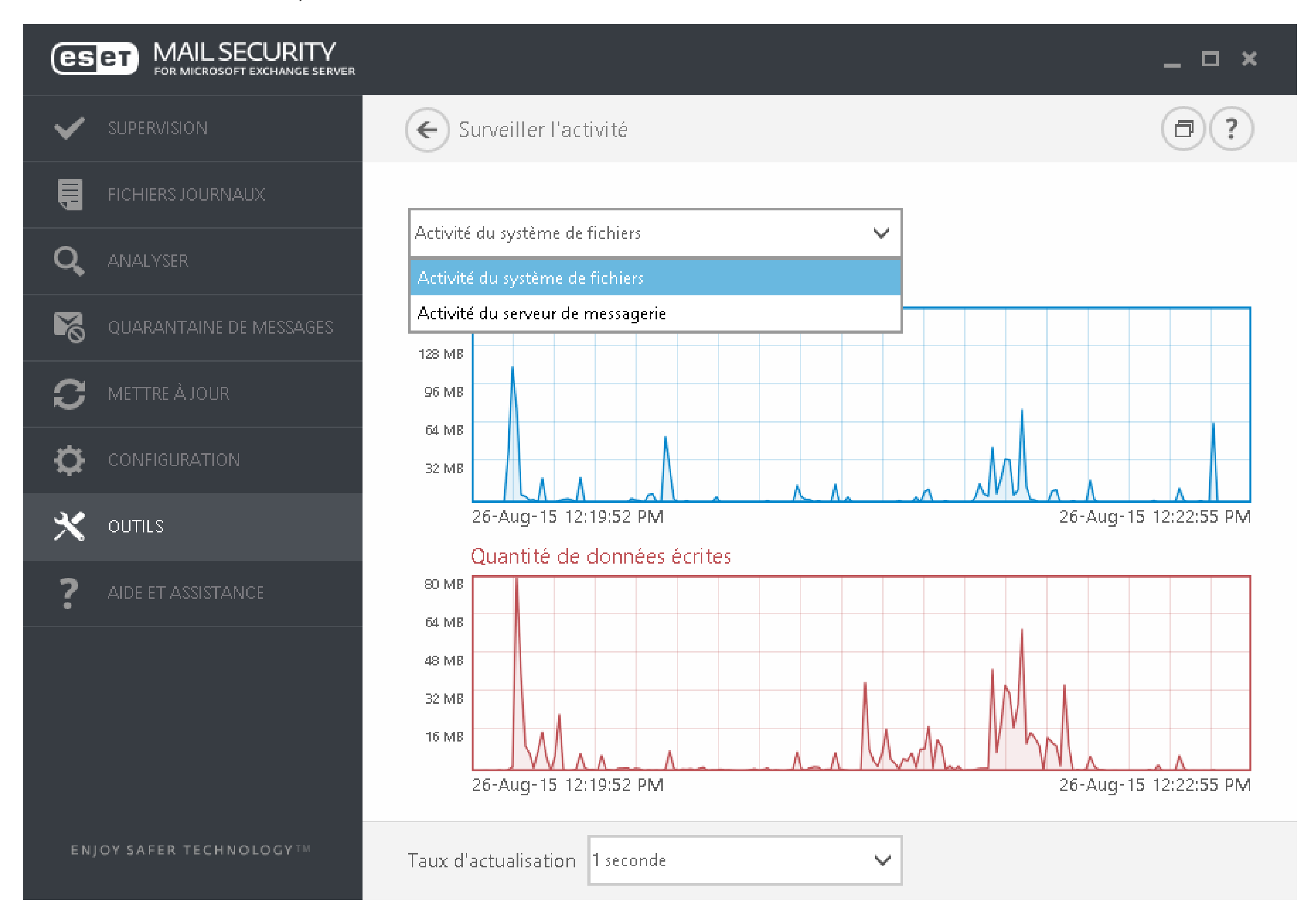
- **Chemin** - Emplacement de l'application sur l'ordinateur.
- **Taille** - Taille du fichier en Ko (kilo-octets) ou Mo (méga-octets).
- **Description** - Caractéristiques du fichier basées sur sa description du système d'exploitation.
- **Réseaux Sociaux** - Nom du fournisseur ou du processus de l'application.
- **Version** - Informations fournies par l'éditeur de l'application.
- **Produit** - Nom de l'application et/ou nom de l'entreprise.
- **Date de création** - Date et heure de création d'une application.
- **Date de modification** - Date et heure de dernière modification d'une application.

REMARQUE : la réputation peut également être vérifiée sur des fichiers qui n'agissent pas en tant que programmes/ processus en cours - Marquez les fichiers que vous souhaitez vérifier, cliquez dessus avec le bouton droit et, dans le menu contextuel, sélectionnez **Options avancées** > **Évaluer la réputation des fichiers à l'aide de ESET Live Grid**.



4.7.2 Surveiller l'activité

Pour voir l'**activité actuelle du système de fichiers** sous forme graphique, cliquez sur **Outils** > **Surveiller l'activité**. Cette option indique la quantité de données lues et écrites dans deux graphiques. Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité du système de fichiers sur la base de l'intervalle sélectionné. Pour modifier l'intervalle, effectuez une sélection dans le menu déroulant **Taux d'actualisation**.



Les options disponibles sont les suivantes :

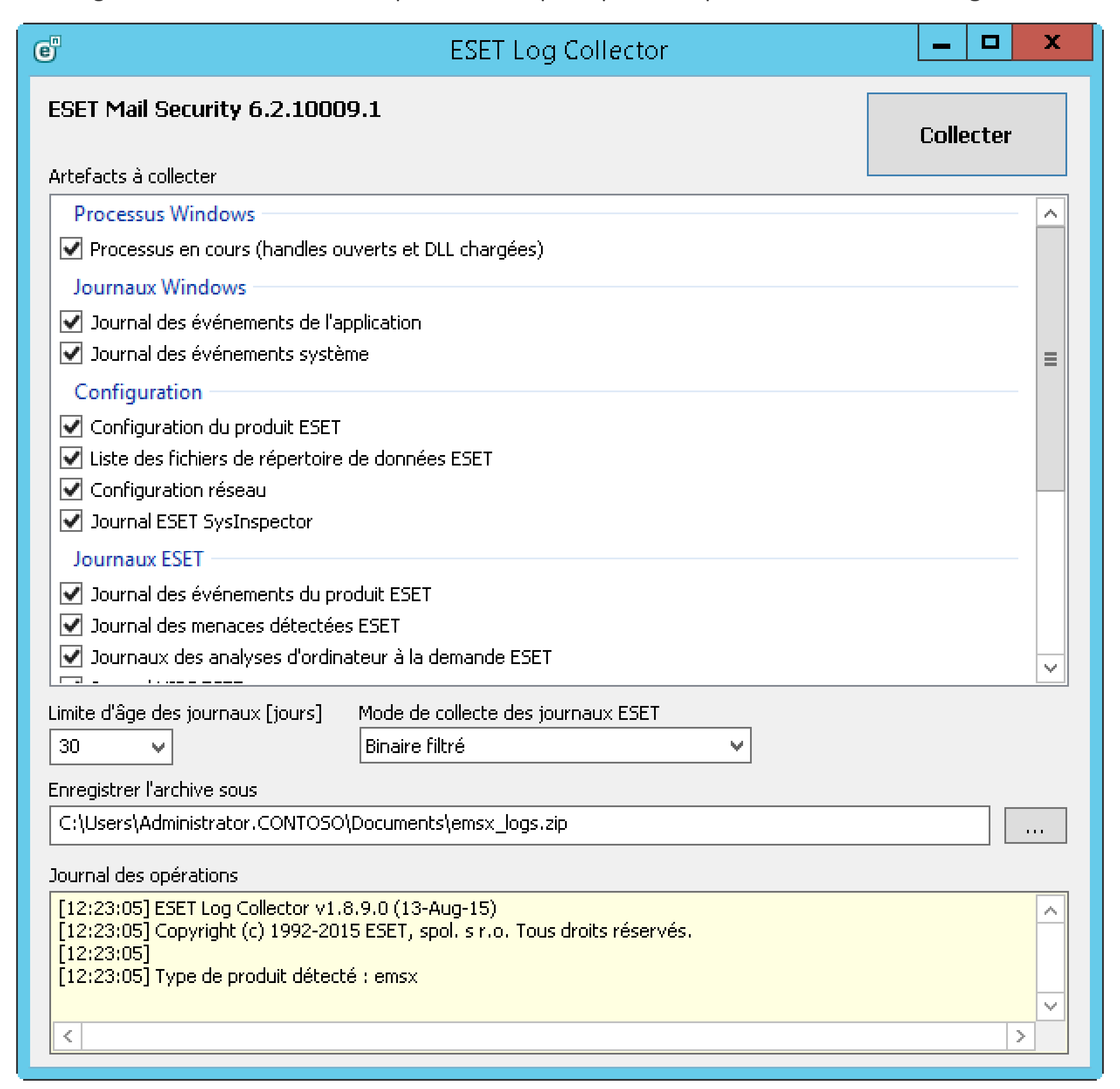
- **1 seconde** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 10 dernières minutes.
- **1 minute (24 dernières heures)** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 24 dernières heures.
- **1 heure (dernier mois)** - Le graphique est actualisé toutes les heures et la chronologie couvre le dernier mois.
- **1 heure (mois sélectionné)** - Le graphique est actualisé toutes les heures et la chronologie couvre le mois sélectionné. Cliquez sur le bouton **Changer de mois** pour effectuer une autre sélection.

L'axe vertical du **graphique d'activité du système de fichiers** représente les données lues (en bleu) et les données écrites (en rouge). Les deux valeurs sont exprimées en Ko (kilo-octets)/Mo/Go. Si vous faites glisser le curseur de la souris sur les données lues ou écrites dans la légende sous le graphique, celui-ci n'affiche que les données relatives à ce type d'activité.

4.7.3 ESET Log Collector

ESET Log Collector est une application qui collecte automatiquement les informations de configuration et les journaux d'un serveur pour permettre de résoudre plus rapidement les problèmes. Lorsque vous signalez un problème auprès du Service client ESET, il se peut que vous deviez fournir les journaux de votre ordinateur. ESET Log Collector facilite la collecte des informations nécessaires.

ESET Log Collector est accessible depuis le menu principal en cliquant sur **Outils** > **ESET Log Collector**.



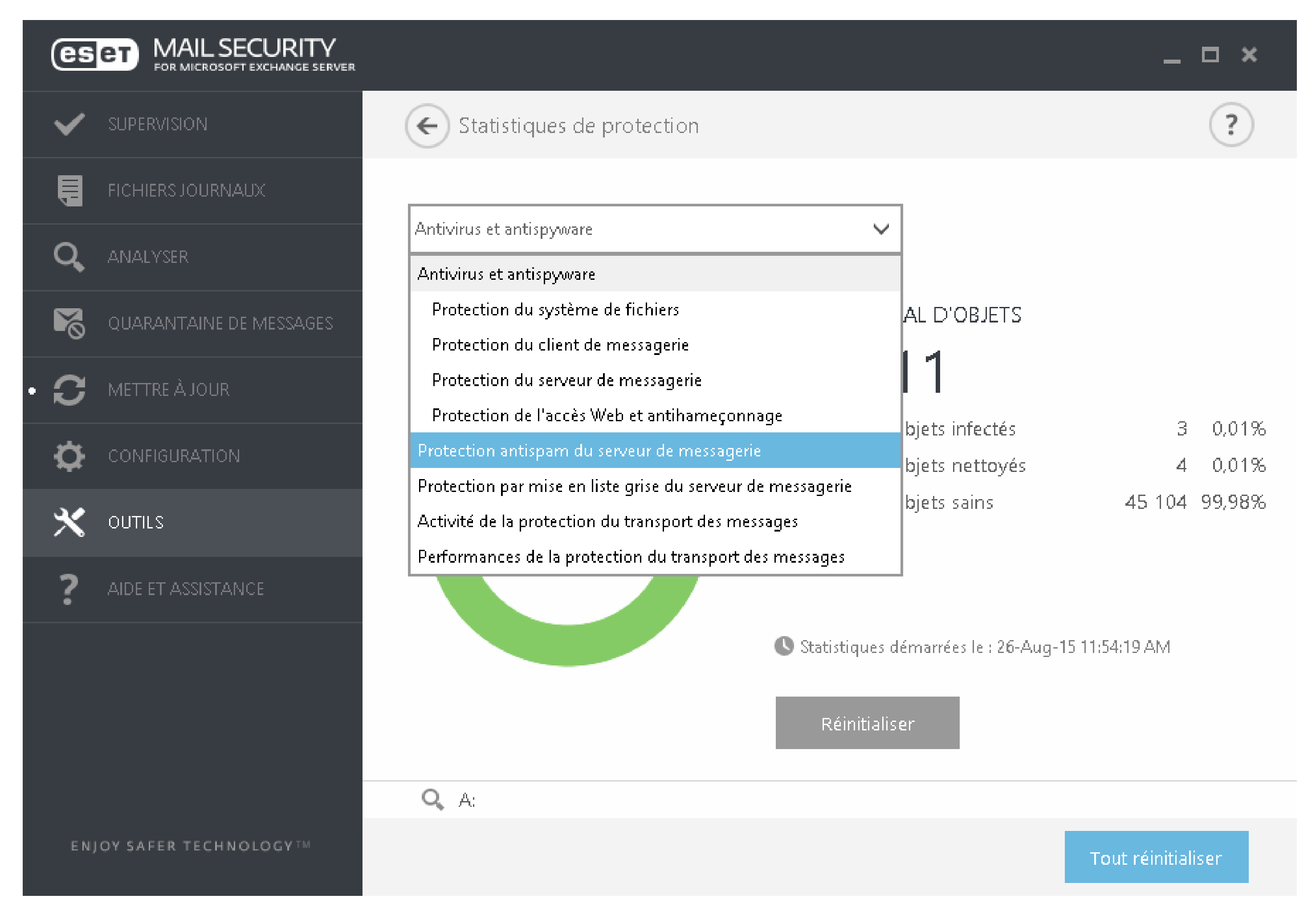
Cochez les cases correspondantes aux journaux que vous souhaitez collecter. Si vous ne savez pas exactement quels journaux sélectionner, laissez toutes les cases cochées (paramètre par défaut). Indiquez l'emplacement où enregistrer les fichiers d'archive, puis cliquez sur **Enregistrer**. Le nom du fichier d'archive est déjà prédéfini. Cliquez sur **Collecter**.

Pendant la collecte, la fenêtre d'opération sur les journaux s'affiche dans la partie inférieure pour que vous puissiez déterminer quelle opération est en cours. Une fois la collecte terminée, tous les fichiers collectés et archivés sont affichés. Cela signifie que la collecte a été correctement effectuée et que le fichier d'archive (par exemple, `emsx_logs.zip`) a été enregistré à l'emplacement indiqué.

Pour plus d'informations sur ESET Log Collector et pour obtenir la liste des fichiers collectés par ESET Log Collector, consultez la base de connaissances ESET.

4.7.4 Statistiques de protection

Pour afficher un graphique des données statistiques relatives aux modules de protection d'ESET Mail Security, cliquez sur **Outils** > **Statistiques de protection**. Dans le menu déroulant **Statistiques**, sélectionnez le module de protection souhaité pour afficher le graphique et la légende correspondants. Placez le pointeur de la souris sur un élément de la légende pour afficher les données de cet élément dans le graphique.



Les graphiques statistiques suivants sont disponibles :

- **Antivirus et antispyware** - Affiche le nombre d'objets infectés et nettoyés.
- **Protection du système de fichiers** - Affiche les objets lus ou écrits dans le système de fichiers.
- **Protection du client de messagerie** - Affiche les objets envoyés ou reçus par les clients de messagerie.
- **Protection du serveur de messagerie** - Affiche les statistiques antivirus et antispyware du serveur de messagerie.
- **Protection de l'accès Web et antihameçonnage** - Affiche uniquement les objets téléchargés par des navigateurs Web.
- **Protection antispam du serveur de messagerie** - Affiche l'historique des statistiques de blocage du courrier indésirable depuis le dernier démarrage.
- **Protection par mise en liste grise du serveur de messagerie** - Inclut les statistiques de blocage du courrier indésirable générées par la méthode de liste grise.
- **Activité de protection du transport des messages** - Affiche les objets vérifiés/bloqués/supprimés par le serveur de messagerie.
- **Performances de la protection du transport des messages** - Affiche les données traitées par VSAPI/l'agent de transport en o/s.
- **Activité de la protection de la base de données de boîtes aux lettres** - Affiche les objets traités par VSAPI (nombre d'objets **vérifiés**, **mis en quarantaine** et **supprimés**).
- **Performances de la protection de la base de données de boîtes aux lettres** - Affiche les données traitées par VSAPI (nombre de moyennes différentes pour **Aujourd'hui**, les **7 derniers jours** et moyennes **depuis la dernière réinitialisation**).

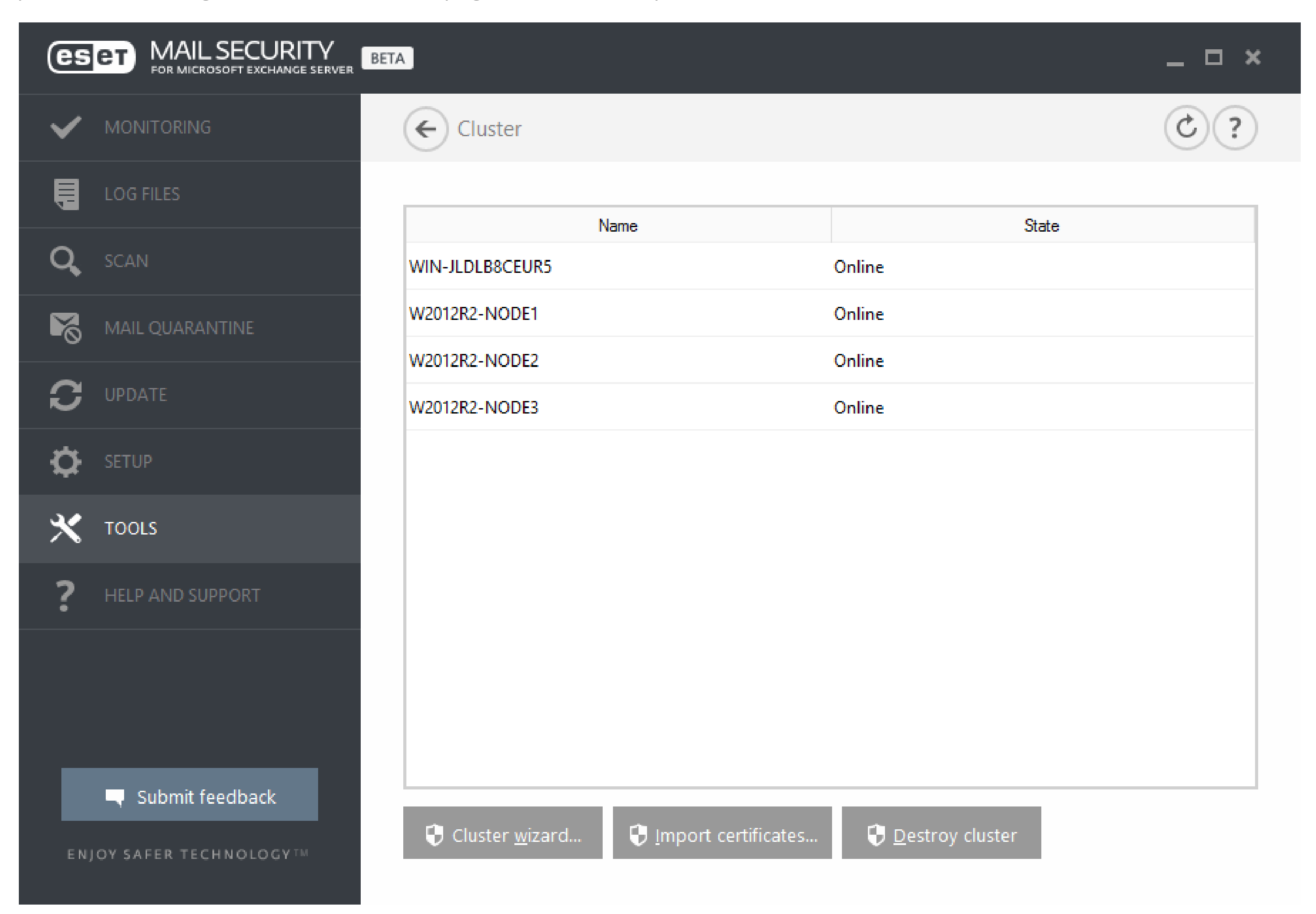
À côté des graphiques statistiques, vous pouvez voir le nombre total d'objets analysés, le nombre d'objets infectés, le nombre d'objets nettoyés et le nombre d'objets propres. Cliquez sur **Réinitialiser** pour effacer les informations de statistiques. Pour effacer et supprimer toutes les données existantes, cliquez sur **Tout réinitialiser**.

4.7.5 Cluster

ESET Cluster est une infrastructure de communication P2P de la gamme des produits ESET pour Microsoft Windows Server.

Cette infrastructure permet aux produits serveur d'ESET de communiquer les uns avec les autres et d'échanger des données (configuration et notifications, par exemple), ainsi que de synchroniser les données nécessaires pour le fonctionnement correct d'un groupe d'instances de produit. Un exemple de ce type de groupe peut être un groupe de nœuds dans un cluster de basculement Windows ou un cluster d'équilibrage de la charge réseau doté d'un produit ESET et dans lequel la configuration du produit doit être identique dans l'ensemble du cluster. ESET Cluster assure cette cohérence entre les instances.

Vous pouvez accéder à la page d'état ESET Cluster dans le menu principal en cliquant sur **Outils** > **Cluster**. Lorsque ce produit est configuré correctement, la page d'état a cet aspect :



Pour configurer ESET Cluster, cliquez sur **Assistant Cluster...**. Pour plus d'informations sur la configuration d'ESET Cluster à l'aide de l'assistant, cliquez ici.

Lors de la configuration d'ESET Cluster, vous pouvez ajouter des nœuds de deux manières : automatiquement à l'aide du cluster de basculement Windows/d'équilibrage de la charge réseau existant ou manuellement en recherchant des ordinateurs se trouvant dans un domaine ou un groupe de travail.

Détection automatique - Détecte automatiquement les nœuds déjà membres d'un cluster de basculement Windows/d'équilibrage de la charge réseau, puis les ajoute à ESET Cluster.
Parcourir - Vous pouvez ajouter manuellement des nœuds en saisissant les noms des serveurs (membres d'un même groupe de travail ou d'un même domaine).

i **REMARQUE :** les serveurs ne doivent pas obligatoirement être membres d'un cluster de basculement Windows/d'équilibrage de la charge réseau pour utiliser la fonctionnalité ESET Cluster. Il n'est pas nécessaire que votre environnement comporte un cluster de basculement Windows/d'équilibrage de la charge réseau pour que vous puissiez utiliser ESET Cluster.

Une fois que vous avez ajouté des nœuds à ESET Cluster, l'étape suivante consiste à installer ESET Mail Security sur chaque nœud. Cette installation est effectuée automatiquement lors de la configuration d'ESET Cluster.

Informations d'identification nécessaires pour une installation à distance d'ESET Mail Security sur d'autres nœuds du cluster :

- Domaine : informations d'identification de l'administrateur du domaine
- Groupe de travail : vous devez veiller à ce que tous les nœuds utilisent les mêmes informations d'identification de compte d'administrateur local

Dans ESET Cluster, vous pouvez également utiliser une combinaison de nœuds automatiquement ajoutés en tant que membres d'un cluster de basculement Windows/d'équilibrage de la charge réseau existant et de nœuds manuellement ajoutés (à condition qu'ils se trouvent dans le même domaine).

i **REMARQUE :** il n'est pas possible de combiner des nœuds de domaine et des nœuds de groupe de travail.

L'utilisation d'ESET Cluster exige également que l'option **Partage de fichiers et d'imprimantes** soit activée dans le Pare-feu Windows avant que l'installation d'ESET Mail Security soit poussée sur les nœuds d'ESET Cluster.

Vous pouvez démanteler ESET Cluster facilement en cliquant sur **Détruire le cluster**. Chaque nœud écrit alors un enregistrement sur la destruction d'ESET Cluster dans son journal des événements. Ensuite, toutes les règles du pare-feu ESET sont supprimées du Pare-feu Windows. Les anciens nœuds reviennent alors à leur état initial et peuvent être réutilisés dans un autre ESET Cluster, si nécessaire.

i **REMARQUE :** la création d'ESET Clusters entre ESET Mail Security et ESET File Security pour Linux n'est pas pris en charge.

L'ajout de nouveaux nœuds à un ESET Cluster existant peut être effectué à tout moment en exécutant l'**Assistant Cluster** comme décrit plus haut et ici.

Consultez la section Cluster pour plus d'informations sur la configuration d'ESET Cluster.

4.7.6 Shell ESET

eShell (abréviation d'ESET Shell) est une interface à ligne de commande pour ESET Mail Security. eShell s'utilise en remplacement de l'interface utilisateur graphique et dispose de toutes les fonctionnalités et options proposées normalement par cette interface. eShell vous permet de configurer et d'administrer l'intégralité du programme sans avoir à utiliser l'interface utilisateur graphique.

Outre les fonctions et fonctionnalités disponible dans l'interface graphique, l'interface à ligne de commande vous permet d'automatiser l'exécution de scripts afin de configurer et de modifier la configuration, ou encore d'effectuer une opération. eShell est également utile pour les utilisateurs qui préfèrent les lignes de commande aux interfaces graphiques.

Le système eShell peut être exécuté de deux manières :

- Mode interactif : ce mode est utile lorsque vous souhaitez utiliser régulièrement eShell (pas simplement exécuter une seule commande), par exemple lorsque vous modifiez la configuration, affichez des journaux, etc. Vous pouvez également utiliser le mode interactif si vous ne connaissez pas encore toutes les commandes. Le mode interactif simplifie la navigation dans eShell. Il affiche également les commandes que vous pouvez utilisez dans un contexte défini.
- Commande unique/mode de traitement par lots : vous pouvez utiliser ce mode si vous avez uniquement besoin d'exécuter une commande sans passer au mode interactif de eShell. Pour ce faire, saisissez dans l'invite de commande Windows `eShell` et ajoutez les paramètres appropriés. Par exemple :

```
eshell get status
```

ou

```
eshell set antivirus status disabled
```

Pour pouvoir exécuter certaines commandes (comme celles du deuxième exemple ci-dessus) en mode de traitement par lots/script, vous devez configurer au préalable certains paramètres. Si vous n'effectuez pas cette configuration, le message **Accès refusé** s'affiche pour des raisons de sécurité.

i **REMARQUE** : Pour bénéficier de toutes les fonctionnalités, ouvrez eShell en utilisant **Exécuter en tant qu'administrateur**. Utilisez la même option lors de l'exécution d'une commande via Windows Command Prompt (cmd). Ouvrez la commande en utilisant **Exécuter en tant qu'administrateur**. Sinon, vous ne serez pas en mesure d'exécuter toutes les commandes. En effet, lorsque vous ouvrez une commande ou eShell en utilisant un compte non-administrateur, vous ne disposez pas des autorisations suffisantes.

i **REMARQUE**: afin d'exécuter les commandes eShell depuis l'invite de commande Windows ou d'exécuter les fichiers de commandes, vous devez effectuer quelques paramétrages. Pour plus d'informations sur l'exécution de fichiers de commandes, cliquez ici.

Pour passer au mode interactif eShell, vous pouvez utiliser l'une des deux méthodes suivantes :

- Par l'intermédiaire du menu Démarrer de Windows : **Démarrer** > **Tous les programmes** > **ESET** > **ESET File Security** > **ESET shell**
- Depuis l'invite de commande Windows en tapant `eShell` et en appuyant sur la touche Entrée.

Lorsque vous exécutez eShell en mode interactif pour la première fois, l'écran de première exécution (guide) s'affiche.

i **REMARQUE** : Si vous souhaitez afficher ultérieurement cet écran de première exécution, tapez la commande `guide` . Il présente des exemples de base concernant l'utilisation d'eShell avec une syntaxe, un préfixe, un chemin d'accès à une commande, des formes abrégées, des alias, etc. Il constitue un guide rapide d'utilisation d'eShell.

À la prochaine exécution d'eShell, cet écran s'affiche :

```
C:\Program Files\ESET\ESET Mail Security\eShell.exe
Copyright (c) 1992-2015 ESET, spol. s r.o. All rights reserved.

Maximum protection

License validity:        12/31/2016
Last successful update: 6/2/2015 4:04:24 PM

Automatic exclusions:                                    Enabled
Anti-Stealth protection:                                 Enabled
Document protection:                                     Disabled
HIPS:                                                    Enabled
Real-time file system protection:                        Enabled
Device control:                                          Disabled
ESET Cluster:                                            Disabled
Presentation mode:                                       Paused
Anti-Phishing protection:                                Enabled
Email client protection:                                 Enabled
Web access protection:                                   Enabled

ABOUT          ANTIVIRUS      DEVICE         GUIDE          INTEGRATION
LICENSE        PASSWORD       RUN            SCHEDULER      SETTINGS
SIGN           STATUS         TOOLS          UI             UPDATE
WEB-AND-EMAIL

eShell>
```

REMARQUE : les commandes ne font pas la distinction entre les majuscules et les minuscules ; que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Personnalisation d'eShell

Vous pouvez personnaliser eShell dans le contexte `ui eshell`. Vous pouvez configurer des alias, des couleurs, la langue et la stratégie d'exécution des scripts. Vous pouvez également choisir d'afficher les commandes masquées et d'autres paramètres.

4.7.6.1 Utilisation

Syntaxe

Pour qu'elles fonctionnent correctement, les commandes doivent avec une syntaxe correcte. Elles peuvent être composées d'un préfixe, d'un contexte, d'arguments, d'options, etc. Voici la syntaxe générale utilisée dans eShell :

[<préfixe>] [<chemin de la commande>] <commande> [<arguments>]

Exemple (cette commande active la protection des documents) :

```
SET ANTIVIRUS DOCUMENT STATUS ENABLED
```

`SET` - préfixe
`ANTIVIRUS DOCUMENT` - chemin vers une commande particulière, contexte auquel la commande appartient
`STATUS` - commande proprement dite
`ENABLED` - argument de la commande

L'utilisation de la valeur `?` en tant qu'argument pour une commande affiche la syntaxe de cette commande. Par exemple, la commande `STATUS ?` affiche la syntaxe de la commande `STATUS` :

SYNTAXE :

```
[get] | status
set status enabled | disabled
```

Vous pouvez constater que `[get]` est entre crochets. Cela indique que le préfixe `get` est l'option par défaut de la commande `status`. En d'autres termes, lorsque vous exécutez la commande `status` sans indiquer de préfixe, la commande utilise le préfixe par défaut (dans ce cas `get status`). Vous gagnerez du temps en n'indiquant pas de préfixe. La valeur `get` est généralement le préfixe par défaut pour la plupart des commandes, mais vous devez effectuer cette vérification pour chaque commande et vous assurer qu'il correspond bien à l'instruction que vous souhaitez exécuter.

REMARQUE : Les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous

saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Préfixe/Opération
Un préfixe est une opération. La commande `GET` fournit des informations sur la configuration d'une fonctionnalité de ESET Mail Security ou indique l'état (`GET ANTIVIRUS STATUS` affiche l'état de la protection en cours). La commande `SET` (préfixe) configure la fonctionnalité ou change son état (`SET ANTIVIRUS STATUS ENABLED` active la protection).

eShell vous permet d'utiliser ces préfixes. Les commandes peuvent prendre en charge ou ne pas prendre en charge les préfixes :

`GET` - renvoie le paramètre/l'état en cours.
`SET` - définit la valeur/l'état.
`SELECT` - sélectionne un élément.
`ADD` - ajoute un élément.
`REMOVE` - supprime un élément.
`CLEAR` - supprime tous les éléments/fichiers.
`START` - démarre une action.
`STOP` - arrête une action.
`PAUSE` - interrompt une action.
`RESUME` - reprend une action.
`RESTORE` - restaure les paramètres/l'objet/le fichier par défaut.
`SEND` - envoie un objet/fichier.
`IMPORT` - importe d'un fichier.
`EXPORT` - exporte dans un fichier.

Les préfixes tels que `GET` et `SET` sont utilisés avec de nombreuses commandes (certaines commandes telles que `EXIT`) n'utilisent pas de préfixe.

Chemin/Contexte de la commande
Les commandes sont placées dans des contextes qui constituent une arborescence. Le niveau supérieur de l'arborescence est la racine. Lorsque vous exécutez eShell, vous vous trouvez au niveau racine :

```
eShell>
```

Vous pouvez exécuter la commande depuis cet emplacement ou saisir le nom du contexte dans l'arborescence pour y accéder. Par exemple, lorsque vous saisissez le contexte `TOOLS` , toutes les commandes et sous-contextes disponibles depuis cet emplacement sont répertoriés.



Les éléments en jaune correspondent aux commandes que vous pouvez exécuter et les éléments en gris sont des sous-contextes que vous pouvez saisir. Un sous-contexte contient des commandes supplémentaires.

Si vous devez remonter d'un niveau, utilisez .. (deux points). Par exemple, imaginons que vous vous trouvez à ce niveau :

```
eShell antivirus startup>
```

saisissez .. et vous remontez d'un niveau :

```
eShell antivirus>
```

Si vous souhaitez retourner au niveau racine depuis `eShell antivirus startup>` (soit deux niveaux en dessous de la racine), tapez simplement .. .. (deux points et deux points séparés par un espace). Vous remontez alors de deux niveaux, ce qui correspond dans ce cas à la racine. Utilisez une barre oblique inverse \ pour retourner directement au niveau racine, quel que soit le niveau auquel vous vous trouvez dans l'arborescence. Si vous souhaitez atteindre un contexte spécifique dans des niveaux supérieurs, utilisez le nombre adéquat de .. pour accéder au niveau souhaité en employant un espace comme séparateur. Si vous souhaitez par exemple remonter de trois niveaux, utilisez .. .. ..

Le chemin est relatif au contexte en cours. Si la commande est contenue dans le contexte en cours, n'indiquez pas de chemin. Par exemple, pour exécuter `GET ANTIVIRUS STATUS` , saisissez :

`GET ANTIVIRUS STATUS` - si vous êtes dans le contexte racine (la ligne de commande indique `eShell>`)
`GET STATUS` - si vous êtes dans le contexte `ANTIVIRUS` (la ligne de commande indique `eShell antivirus>`)
`.. GET STATUS` - si vous êtes dans le contexte `ANTIVIRUS STARTUP` (la ligne de commande indique `eShell antivirus startup>`)

REMARQUE : vous pouvez utiliser un point (.) au lieu de deux (..), car un point est l'abréviation de deux points. Par exemple :

`. GET STATUS` - si vous êtes dans le contexte `ANTIVIRUS STARTUP` (la ligne de commande indique `eShell antivirus startup>`)

Argument
Un argument est une action qui peut être réalisée pour une commande particulière. Par exemple, la commande `CLEAN-LEVEL` (située dans `ANTIVIRUS REALTIME ENGINE`) peut être utilisée avec les arguments suivants :

`no` - Pas de nettoyage
`normal` - Nettoyage normal
`strict` - Nettoyage strict

Les arguments `ENABLED` ou `DISABLED`permettent d'activer ou de désactiver une fonctionnalité.

Forme abrégée/Commandes raccourcies
eShell vous permet de raccourcir les contextes, les commandes et les arguments (à condition que l'argument soit un paramètre ou une autre option). Il n'est pas possible de raccourcir un préfixe ou un argument s'il s'agit d'une valeur concrète telle qu'un nombre, un nom ou un chemin.

Voici des exemples de forme raccourcie :

`set status disabled` => `set stat en`
`add antivirus common scanner-excludes C:\path\file.ext` => `add ant com scann C:\path\file.ext`

Si deux commandes ou contextes commencent par la même lettre, `ABOUT` et `ANTIVIRUS`, et que vous saisissez la commande raccourcie `A` , eShell ne parvient pas à déterminer laquelle de ces deux commandes vous souhaitez exécuter. Un message d'erreur s'affiche et répertorie les commandes commençant par un « A » pour que vous puissiez sélectionner celle à exécuter :

```
eShell>a
La commande suivante n'est pas unique : a

Les commandes suivantes sont disponibles dans ce contexte :
 ABOUT - Affiche les informations sur le programme
 ANTIVIRUS - Passe au contexte antivirus
```

Ensuite, l'ajout d'une ou de plusieurs lettres (AB au lieu de A) eShell exécute la commande ABOUT car cette commande est unique.

REMARQUE : afin d'avoir la garantie qu'une commande s'exécute comme vous le souhaitez, il est recommandé de ne pas abréger les commandes, les arguments, etc. et d'utiliser plutôt la forme complète. La commande s'exécute alors exactement comme vous le souhaitez et vous évite de commettre des erreurs. Ce conseil s'applique notamment pour les fichiers et les scripts de traitement par lots.

Saisie semi-automatique
Il s'agit d'une nouvelle fonctionnalité d'eShell (ajoutée dans la version 2.0). Elle ressemble beaucoup à la fonctionnalité de saisie semi-automatique de l'invite de commande Windows. Alors que l'invite de commande Windows effectue une saisie semi-automatique des chemins d'accès aux fichiers, eShell effectue également une saisie semi-automatique des noms de commande, de contexte et d'opération. La saisie semi-automatique des arguments n'est pas prise en charge. Lorsque vous tapez une commande, appuyez sur la touche TAB pour terminer la saisie ou parcourir les variantes disponibles. Appuyez sur MAJ+TAB pour parcourir les variantes dans le sens inverse. Le mélange d'une forme abrégée et de la saisie semi-automatique n'est pas pris en charge. Utilisez une de ces deux options. Par exemple, lorsque vous saisissez `antivir real scan` la frappe de la touche TAB ne donne aucun résultat. Saisissez plutôt `antivir` et appuyez sur la touche TAB pour saisir automatiquement `antivirus`, tapez ensuite real + TAB et scan + TAB. Vous pouvez ensuite parcourir toutes les variantes disponibles : scan-create, scan-execute, scan-open, etc.

Alias
Un alias est un autre nom qui peut être utilisé pour exécuter une commande (à condition que la commande dispose d'un alias). Voici quelques alias par défaut :

`(global) close` - exit
`(global) quit` - exit
`(global) bye` - exit
`warnlog` - tools log events
`virlog` - tools log detections
`antivirus on-demand log` - tools log scans

"(global)" signifie que la commande peut être utilisée dans tous les emplacements, quel que soit le contexte actuel. Une commande peut comporter plusieurs alias. Par exemple, la commande EXIT comporte les alias CLOSE, QUIT et BYE. Si vous souhaitez quitter eShell, vous pouvez utiliser la commande EXIT proprement dite ou l'un de ses alias. L'alias VIRLOG est attribué à la commande DETECTIONS qui se trouve dans le contexte TOOLS LOG . Les détections de commande sont ainsi disponibles depuis le contexte ROOT , ce qui facilite l'accès (vous n'avez plus à saisir TOOLS puis le contexte LOG et l'exécuter directement depuis ROOT).

eShell vous permet de définir vos propres alias. Commande ALIAS est accessible dans le contexte UI ESHELL .

Paramètres protégés par mot de passe
Les paramètres de ESET Mail Security peuvent être protégés par mot de passe. Vous pouvez définir un mot de passe à l'aide de l'interface graphique utilisateur ou d'eShell à l'aide de la commande `set ui access lock-password` . Vous devez ensuite saisir ce mot de passe de manière interactive pour certaines commandes (comme celles qui permettent de modifier des paramètres ou des données). Si vous envisagez d'utiliser eShell pendant une longue période et si vous ne souhaitez pas saisir le mot de passe de manière répétée, vous pouvez faire en sorte qu'eShell mémorise le mot de passe à l'aide de la commande `set password` . Votre mot de passe est alors automatiquement saisi pour chaque commande exécutée qui le demande. Le mot de passe est mémorisé jusqu'à ce que vous quittiez eShell. Vous devez donc réutiliser la commande `set password` lorsque vous démarrez une nouvelle session et que vous souhaitez qu'eShell mémorise le mot de passe.

Guide / Aide
Lorsque vous exécutez la commande GUIDE ou HELP , l'écran de première exécution apparaît et vous explique comment utiliser eShell. Cette commande est disponible dans le contexte ROOT (`eShell>`).

Historique de commande
eShell conserve un historique des commandes exécutées. Cet historique s'applique uniquement à la session interactive eShell en cours. Lorsque vous quittez eShell, l'historique des commandes est supprimé. Utilisez les flèches Haut et Bas de votre clavier pour parcourir l'historique. Lorsque vous avez localisé la commande que vous

recherchiez, vous pouvez la réexécuter ou la modifier sans avoir à saisir l'intégralité de la commande depuis le début.

CLS/Effacement de l'écran
La commande `CLS` peut être utilisée pour effacer le contenu de l'écran. Cette commande fonctionne de la même manière que l'invite de commande Windows ou que toute autre interface à ligne de commande.

EXIT/CLOSE/QUIT/BYE
Pour fermer ou quitter eShell, vous pouvez utiliser l'une de ces commandes (`EXIT`, `CLOSE`, `QUIT` ou `BYE`).

4.7.6.2 Commandes

Cette section répertorie quelques commandes eShell de base, ainsi qu'une description en guise d'exemple.

REMARQUE : Les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Exemples de commandes (contenues dans le contexte ROOT) :

ABOUT

Répertorie les informations sur le programme. Cette commande indique le nom du produit installé, son numéro de version, les composants installés (notamment le numéro de version de chaque composant), ainsi que des informations de base sur le serveur et le système d'exploitation sur lesquels s'exécute ESET Mail Security.

CHEMIN DE CONTEXTE :

```
root
```

PASSWORD

Normalement, lorsque vous exécutez des commandes protégées par mot de passe, vous êtes invité à taper un mot de passe pour des raisons de sécurité. Il concerne les commandes qui désactivent la protection antivirus et qui peuvent avoir une incidence sur le fonctionnement du produit ESET Mail Security. Vous êtes invité à saisir un mot de passe chaque fois que vous exécutez une commande de ce type. Afin d'éviter d'avoir à saisir un mot de passe à chaque fois, vous pouvez définir ce mot de passe. Il sera mémorisé par eShell et utilisé automatiquement à chaque exécution d'une commande protégée par un mot de passe. De cette manière, vous n'aurez plus à le saisir à chaque fois.

REMARQUE : le mot de passe défini ne fonctionne que pour la session interactive eShell en cours. Lorsque vous quittez eShell, ce mot de passe défini est supprimé. Lorsque vous redémarrez eShell, le mot de passe doit être redéfini.

Ce mot de passe défini est également très utile lorsque vous exécutez des fichiers/scripts de traitement par lots. Voici un exemple de fichier de traitement par lots :

```
eshell start batch "&" set password plain <votremotdepasse> "&" set status disabled
```

La commande concaténée ci-dessus démarre un mode de traitement par lots, définit le mot de passe qui sera utilisé et désactive la protection.

CHEMIN DE CONTEXTE :

```
root
```

SYNTAXE :

```
[get] | restore password

set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou efface le mot de passe

`restauration` - Efface le mot de passe

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre.

`password` - Mot de passe.

EXEMPLES :

`set password plain <votremotdepasse>` - Définit un mot de passe qui sera utilisé pour les commandes protégées par mot de passe.

`restore password` - Efface le mot de passe.

EXEMPLES :

`get password` - Utilisez cette commande pour définir si le mot de passe est configuré (le mot de passe n'apparaît pas clairement ; il est remplacé par une série d'astérisques *). Si vous ne voyez aucun astérisque, cela signifie qu'aucun mot de passe n'est défini.

`set password plain <votremotdepasse>` - Utilisez cette commande pour configurer le mot de passe défini

`restore password` - Cette commande efface le mot de passe défini.

STATUS

Affiche des informations sur l'état en cours de la protection ESET Mail Security (identique à l'interface utilisateur graphique).

CHEMIN DE CONTEXTE :

`root`

SYNTAXE :

`[get] | restore status`

`set status disabled | enabled`

OPÉRATIONS :

`get` - Affiche l'état de la protection antivirus

`set` - Désactive/Active la protection antivirus

`restore` - Restaure les paramètres par défaut

ARGUMENTS :

`disabled` - Désactive la protection antivirus

`enabled` - Active la protection antivirus

EXEMPLES :

`get status` - Affiche l'état de la protection en cours

`set status disabled` - Désactive la protection

`restore status` - Restaure la protection sur le paramètre par défaut (activée)

VIRLOG

Cette commande est un alias de la commande `DETECTIONS` . Elle est utile lorsque vous devez afficher des

informations sur les infiltrations détectées.

WARNLOG

Cette commande est un alias de la commande `EVENTS` . Elle est utile lorsque vous devez afficher des informations sur différents événements.

4.7.6.3 Fichiers de commandes/scripts

Vous pouvez utiliser eShell comme outil de création de scripts puissant pour l'automatisation. Pour utiliser un fichier de commandes dans eShell, créez-en un comportant un eShell et une commande. Par exemple :

```
eshell get antivirus status
```

Vous pouvez également créer une chaîne de commandes, ce qui est parfois nécessaire. Si vous souhaitez par exemple obtenir le type d'une tâche planifiée spécifique, saisissez la commande suivante :

```
eshell select scheduler task 4 "&" get scheduler action
```

La sélection d'un élément (tâche numéro 4 dans le cas présent) ne s'applique généralement qu'à une instance d'eShell en cours d'exécution. Si vous deviez exécuter ces commandes à la suite, la seconde commande échouerait en affichant l'erreur « Aucune tâche n'est sélectionnée ou la tâche sélectionnée n'existe plus. »

Pour des raisons de sécurité, la stratégie d'exécution est définie par défaut sur Scripts limités. Vous pouvez ainsi utiliser eShell comme outil de surveillance (dans ce cas, vous ne pouvez pas apporter de modifications à la configuration de ESET Mail Security). Si vous utilisez des commandes qui ont un impact sur la sécurité, comme la désactivation de la protection, le message **Accès refusé** s'affiche. Pour pouvoir exécuter ces commandes qui apportent des modifications de configuration, il est recommandé d'utiliser des fichiers de commandes signés.

Si vous devez, pour une raison spécifique, modifier la configuration à l'aide d'une commande saisie manuellement dans l'invite de commande, vous devez accorder un accès total à eShell (non recommandé). Pour accorder un accès total, utilisez la commande `ui eshell shell-execution-policy` en mode interactif d'eShell. Vous pouvez également accorder un accès total par le biais de l'interface graphique utilisateur dans **Configuration avancée** > **Interface utilisateur** > ESET Shell.

Fichiers de commandes signés
eShell vous permet de protéger les fichiers de commandes courants (*.bat) à l'aide d'une signature. Les scripts sont signés à l'aide du mot de passe utilisé pour la protection des paramètres. Pour signer un script, vous devez activer au préalable la protection des paramètres. Vous pouvez le faire dans l'interface graphique utilisateur ou dans eShell à l'aide de la commande `set ui access lock-password` . Une fois que le mot de passe de protection des paramètres est configuré, vous pouvez commencer à signer les fichiers de commandes.

Pour signer un fichier de commandes, exécutez `sign <script.bat>` à partir du contexte racine d'eShell, où *script.bat* correspond au chemin d'accès au script à signer. Saisissez le mot de passe qui sera utilisé pour la signature, puis confirmez-le. Ce mot de passe doit correspondre au mot de passe de protection des paramètres. La signature est placée dans la partie inférieure du fichier de commandes sous forme de commentaire. Si le script a déjà été signé, sa signature est remplacée par la nouvelle.

i **REMARQUE** : lorsque vous modifiez un fichier de commandes signé, vous devez le resigner.

i **REMARQUE** : si vous modifiez le mot de passe de protection des paramètres, vous devez resigner tous les scripts (sinon, les scripts ne peuvent plus être exécutés), car le mot de passe saisi lors de la signature d'un script doit correspondre au mot de passe de protection des paramètres sur le système cible.

Pour exécuter un fichier de commandes signé à partir de l'invite de commande Windows ou en tant que tâche planifiée, utilisez la commande suivante :

```
eshell run <script.bat>
```

, où script.bat correspond au chemin d'accès au fichier de commandes Par exemple : `eshell run d:\myeshellscript.bat`

4.7.7 ESET SysInspector

ESET SysInspector est une application qui inspecte méticuleusement votre ordinateur, réunit des informations détaillées sur les composants système, tels que pilotes et applications installés, connexions réseau ou entrées de registre importantes, puis évalue le niveau de risque de chaque composant. Ces informations peuvent aider à déterminer la cause d'un comportement suspect du système pouvant être dû à une incompatibilité logicielle ou matérielle, ou à une infection par un logiciel malveillant.

La fenêtre ESET SysInspector affiche les informations suivantes relatives aux journaux créés :

- **Heure** - Heure de création du journal.
- **Commentaire** - Bref commentaire.
- **Utilisateur** - Nom de l'utilisateur qui a créé le journal.
- **État** - État de création du journal.

Les actions disponibles sont les suivantes :

- **Ouvrir** - Ouvre le journal créé. Vous pouvez également cliquer avec le bouton droit sur le journal créé et sélectionner **Afficher** dans le menu contextuel.
- **Comparer** - Compare deux journaux existants.
- **Créer** - Crée un journal. Veuillez patienter jusqu'à ce que le journal ESET SysInspector soit prêt (l'option **État** indique Créé).
- **Supprimer** - Supprime les journaux sélectionnés de la liste.

En cliquant avec le bouton droit de la souris sur un ou plusieurs journaux sélectionnés, vous ouvrez un menu contextuel qui donne accès aux options suivantes :

- **Afficher** - Ouvre le journal sélectionné dans ESET SysInspector (équivaut à double-cliquer sur un journal).
- **Créer** - Crée un journal. Veuillez patienter jusqu'à ce que le journal ESET SysInspector soit prêt (l'option **État** indique Créé).
- **Supprimer tout** - Supprime tous les journaux.
- **Exporter** - Exporte le journal dans un fichier *.xml* ou *.xml* compressé.

4.7.7.1 Créer un rapport de l'état de l'ordinateur

Entrez un bref commentaire décrivant le journal à créer, puis cliquez sur le bouton **Ajouter**. Patientez jusqu'à ce que le journal d'ESET SysInspector soit prêt (état Créé). Selon la configuration matérielle et les données système, la création du journal peut prendre un certain temps.

4.7.7.2 ESET SysInspector

4.7.7.2.1 Introduction à ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche en détail toutes les données obtenues. Des informations telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

Vous pouvez accéder à ESET SysInspector de deux manières : Depuis la version intégrée dans les solutions ESET Security ou en téléchargeant gratuitement la version autonome (SysInspector.exe) depuis le site Internet d'ESET. Les deux versions sont identiques en matière de fonctionnalités et disposent des mêmes contrôles de programme. La seule différence réside dans la façon dont les résultats sont gérés. Les versions autonomes et intégrées vous permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée vous permet également de stocker vos instantanés système directement dans **Outils** > **ESET SysInspector** (excepté ESET Remote Administrator).

Veuillez patienter pendant que ESET SysInspector analyse votre ordinateur. L'analyse peut prendre entre 10 secondes et quelques minutes, en fonction de la configuration de votre matériel, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

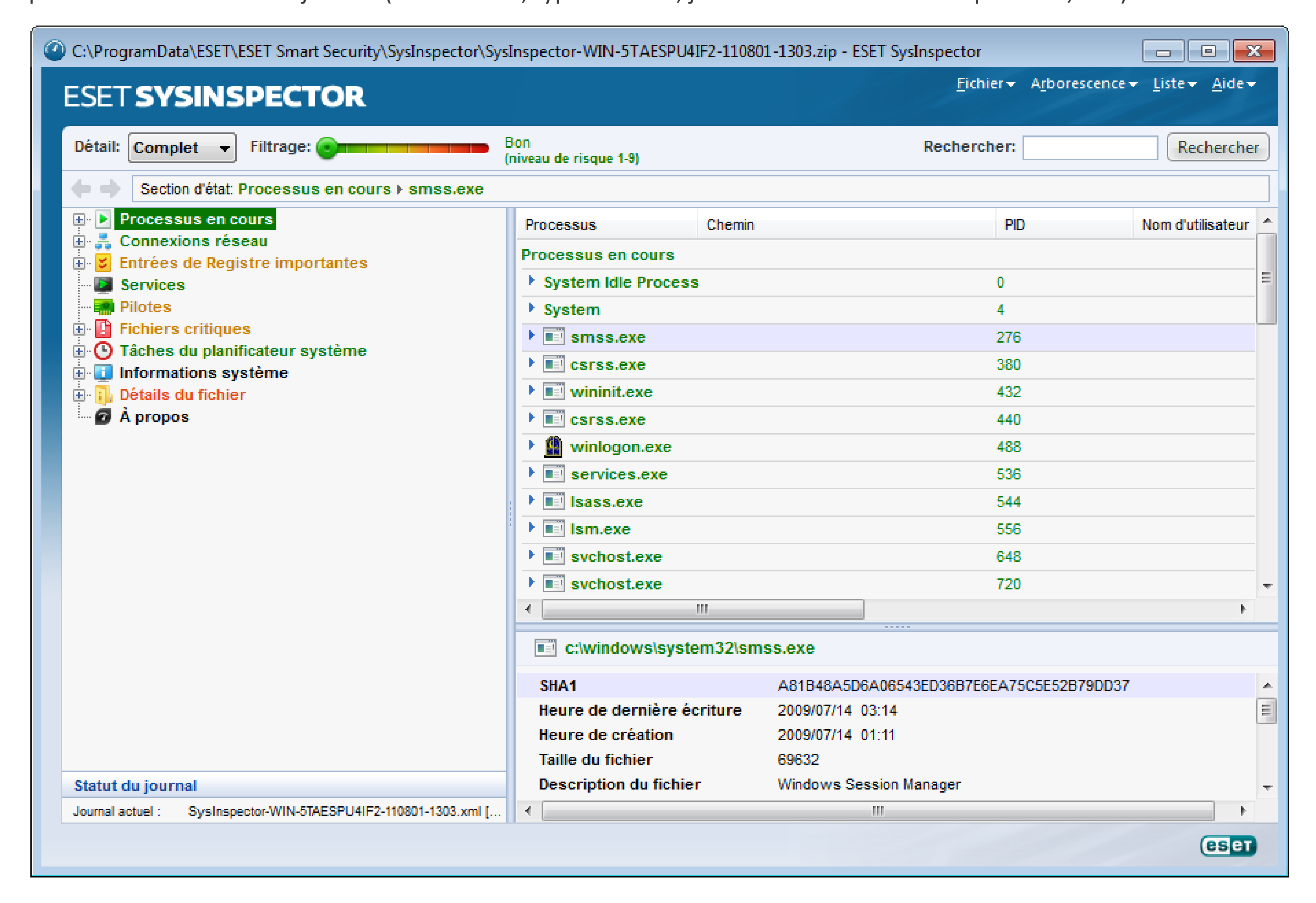
4.7.7.2.1.1 Démarrage d'ESET SysInspector

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site Web d'ESET.

Patientez pendant que l'application vérifie le système, une opération qui pourrait durer plusieurs minutes en fonction du matériel et des données à recueillir.

4.7.7.2.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale est divisée en quatre principales sections : les Contrôles du programme situés dans le haut de la fenêtre principale, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails à droite au bas de la fenêtre principale. La section État du journal énumère les paramètres de base d'un journal (filtre utilisé, type de filtre, journal résultat d'une comparaison, etc.).



4.7.7.2.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

Fichier

En cliquant sur **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

REMARQUE : vous pouvez ouvrir des rapports enregistrés de ESET SysInspector en les faisant glisser et en les déposant sur la fenêtre principale.

Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de

service.

Liste

Contient des fonctions qui simplifient la navigation dans le programme, ainsi que d'autres fonctionnalités comme l'obtention d'informations en ligne.

Aide

Contient des informations sur l'application et ses fonctions.

Détails

Ce paramètre détermine les informations affichées dans la fenêtre principale afin de simplifier l'utilisation des informations. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode Moyen, le programme affiche moins de détails. En mode Complet, ESET SysInspector indique toutes les informations requises pour résoudre des problèmes très particuliers.

Filtrage des éléments

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de Registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Si le curseur est positionné tout à fait à gauche (Niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments qui sont plus suspects que le niveau affiché. Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments qui appartiennent aux catégories de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas certaines des solutions de sécurité d'ESET, nous vous conseillons d'analyser votre système à l'aide d'ESET Online Scanner dans le cas où ESET SysInspector détecte un élément de ce genre. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé grâce à la couleur que prend le curseur pour indiquer le niveau de risque.

Rechercher

La fonction de recherche permet de trouver rapidement un élément sur la base de son nom ou d'une partie de son nom. Les résultats de la recherche sont affichés dans la fenêtre Description.

Retour

En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur les flèches arrière ou avant.

Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

Important : les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

4.7.7.2.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections principales baptisées nœuds. Si des détails supplémentaires sont disponibles, vous pouvez les afficher en développant chaque nœud en sous-nœuds. Pour développer ou réduire un nœud, double-cliquez sur son nom, ou cliquez sur ⊞ ou sur ⊟ en regard du nom du nœud. Quand vous parcourez la structure arborescente des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

Processus en cours

Ce nœud comprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails comprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application et le niveau de risque du fichier.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

REMARQUE : Un système d'exploitation comprend plusieurs composants noyaux importants fonctionnant 24 h. sur 24/7 j. sur 7 et assurant des fonctions de base et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles garantissent l'optimisation préalable au lancement pour ce processus ; ils ne présentent aucun danger pour le système.

Connexions de réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

Entrées de Registre importantes

Contient la liste des entrées de Registre sélectionnées qui sont souvent liées à des problèmes système. Il s'agit des entrées qui indiquent les applications de démarrage, les objets d'application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de Registre particulières. La fenêtre Détails peut également présenter des détails supplémentaires.

Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez contrôler la manière dont le démarrage du service est paramétré, ainsi que des détails spécifiques du fichier dans la fenêtre Détails.

Pilotes

Liste des pilotes installés sur le système.

Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Tâches du planificateur système

Contient une liste de tâches déclenchées par le Planificateur de tâches de Windows à une heure précise ou selon un intervalle spécifié.

Informations système

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement définies, les droits de l'utilisateur et les journaux d'événements du système.

Détails du fichier

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

À propos de

Informations sur la version de ESET SysInspector et la liste des modules du programme.

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

Générer

Ctrl+G	génère un instantané standard du statut de l'ordinateur
Ctrl+H	génère un instantané du statut de l'ordinateur qui peut également journaliser des informations sensibles

Filtrage des éléments

1, O	affiche les éléments de niveau de risque 1 à 9 (acceptable)
2	affiche les éléments de niveau de risque 2 à 9 (acceptable)
3	affiche les éléments de niveau de risque 3 à 9 (acceptable)
4, U	affiche les éléments de niveau de risque 4 à 9 (inconnu)
5	affiche les éléments de niveau de risque 5 à 9 (inconnu)
6	affiche les éléments de niveau de risque 6 à 9 (inconnu)
7, B	affiche les éléments de niveau de risque 7 à 9 (risqué)
8	affiche les éléments de niveau de risque 8 à 9 (risqué)
9	affiche les éléments de niveau de risque 9 (risqué)
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+0	mode de filtrage, niveau égal uniquement

Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	afficher tous les détails
Ctrl+2	afficher les détails de précision moyenne
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	accède à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément

Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison
Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés ; le journal indique les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés ; le journal indique les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

4.7.7.2.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Cet outil est utile si vous souhaitez assurer le suivi des modifications dans le système. Il vous permettra de détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Accédez au menu **Fichier** > **Enregistrer le journal** pour enregistrer le journal dans un fichier. Vous pouvez ouvrir et afficher les fichiers journaux ultérieurement. Pour ouvrir un journal existant, sélectionnez **Fichier** > **Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

En comparant deux journaux, vous pouvez afficher un journal actif et un autre journal enregistré dans un fichier. Pour comparer des journaux, choisissez l'option **Fichier** > **Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné est comparé au journal actif dans les fenêtres principales de l'application. Le journal comparatif n'indiquera que les différences entre ces deux journaux.

REMARQUE : si vous comparez deux fichiers journaux, choisissez **Fichier** > **Enregistrer le journal** pour l'enregistrer dans un fichier ZIP. Les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

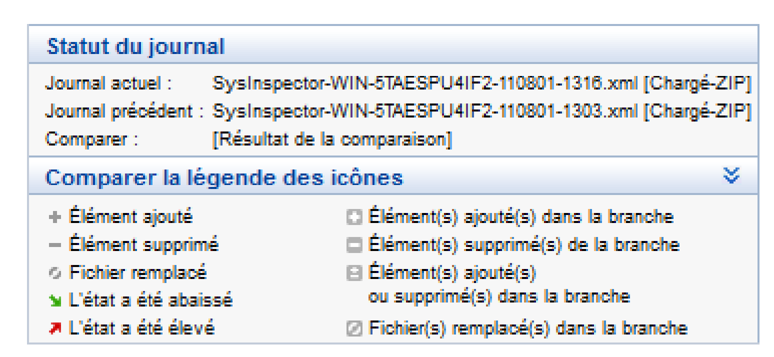
En regard des éléments affichés, ESET SysInspector ajoute des symboles qui identifient les différences entre les journaux comparés.

Les éléments marqués par – se trouvent uniquement dans le journal actif et sont absents du journal de comparaison ouvert. Les éléments marqués du signe + ne figurent que dans le journal ouvert et sont absents du journal actif.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- cette section de l'arborescence contient de nouvelles valeurs.
- – valeur supprimée, présente uniquement dans le journal précédent.
- cette section de l'arborescence contient des valeurs supprimées.
- valeur/fichier modifié.
- cette section de l'arborescence contient des valeurs/fichiers modifiés.
- le niveau de risque a diminué/était supérieur dans le journal précédent.
- le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.



Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts ultérieurement :

Exemple

Générez et enregistrez un journal contenant des informations d'origine concernant le système, dans un fichier nommé précédent.xml. Après avoir apporté des modifications au système, ouvrez ESET SysInspector et laissez-le générer un nouveau journal. Enregistrez ce journal sous le nom *actuel.xml*.

Pour voir les différences entre ces deux journaux, utilisez l'option **Fichier** > **Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

SysInspector.exe actuel.xml précédent.xml

4.7.7.2.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

/gen	crée un journal directement depuis la ligne de commande sans exécuter l'interface utilisateur.
/privacy	crée un journal qui exclut les informations sensibles.
/zip	stocke le journal obtenu directement sur le disque dans un fichier compressé.
/silent	supprime l'affichage de la barre de progression de la création du journal.
/help, /?	affiche des informations sur les paramètres de la ligne de commande.

Exemples

Pour charger un journal en particulier directement dans le navigateur, saisissez : *SysInspector.exe "c:\clientlog.xml"*
Pour créer un journal à l'emplacement actuel, saisissez : *SysInspector.exe /gen*
Pour créer un journal dans un dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\"*
Pour créer un journal dans un fichier/dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier \monnouveaujournal.xml"*
Pour créer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : *SysInspector.exe /gen="c:\monnouveaujournal.zip"/privacy/zip*
Pour comparer deux journaux, utilisez : *SysInspector.exe "actuel.xml" "original.xml"*

REMARQUE : si le nom du fichier/dossier contient un espace, saisissez-le entre guillemets.

4.7.7.2.4 Script de service

Le script de service est un outil qui vise à offrir une aide aux clients qui utilisent ESET SysInspector en supprimant les objets indésirables du système.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou des parties sélectionnées uniquement. Après l'exportation, vous pouvez marquer des objets indésirables pour suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications non qualifiées peuvent endommager le système d'exploitation.

Exemple

si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

- Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
- Sélectionnez le premier élément de la section à gauche (dans l'arborescence), appuyez sur la touche Ctrl, puis sélectionnez le dernier élément afin de marquer tous les éléments.
- Cliquez avec le bouton droit sur les objets sélectionnés, puis sélectionnez l'option du menu contextuel **Exporter les sections sélectionnées dans un script de service**.
- Les objets sélectionnés sont exportés dans un nouveau journal.
- Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut + par - pour tous les objets que vous souhaitez supprimer. Assurez-vous que vous n'avez sélectionné aucun fichier/objet important du système d'exploitation.
- Ouvrez ESET SysInspector, cliquez sur **Fichier** > **Exécuter le script de services** entrez le chemin d'accès de votre script.
- Cliquez sur **OK** pour lancer le script.

4.7.7.2.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

REMARQUE : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

4.7.7.2.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut pas être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (elles indiquent les éléments qui sont traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC, puis par son code de hachage CRC16 entre astérisques (*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le processus s'arrête à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section répertorie la liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module et les arrête.

03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lorsque le script est exécuté, il localise le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

05) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées sont supprimées à l'exécution du script.

06) Important registry entries (entrées de Registre importantes)

Cette section contient des informations relatives aux entrées de Registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur leur valeur par défaut lors de l'exécution du script. L'action à appliquer à chaque entrée dépend de la catégorie de l'entrée et de la valeur de la clé dans ce Registre.

07) Services (services)

Cette section répertorie les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés après l'exécution du script.

08) Drivers (pilotes)

Cette section répertorie les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés sont arrêtés. Notez que certains pilotes n'autoriseront pas leur arrêt.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers essentiels au système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés sont soit supprimés, soit restaurés sur leur valeur d'origine.

4.7.7.2.4.3 Exécution des scripts de services

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de services** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ?** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître pour vous indiquer que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirmera l'exécution du script.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaît : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui répertorie les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue apparaîtra avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts non signés et inconnus peut endommager gravement les données de votre ordinateur. Voulez-vous vraiment exécuter le script et ses actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête endommagé, titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

4.7.7.2.5 FAQ

L'exécution d'ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien que ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraîne la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour en enregistrer un, dans le menu principal, sélectionnez **Fichier** > **Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut, les fichiers sont enregistrés dans le répertoire *%USERPROFILE%\Mes documents*, conformément à la convention de dénomination de fichier SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML. Vos pouvez changer l'emplacement et le nom du fichier avant la sauvegarde si vous le souhaitez.

Comment puis-je consulter le fichier journal d'ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier** > **Ouvrir le journal** dans le menu principal. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET SysInspector, il est

conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peuvent désactiver la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format de fichier journal ? Existe-t-il un kit de développement logiciel (SDK) ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal, ni SDK car le programme en est toujours au stade du développement. Après la diffusion du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de Registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Sur la base de cette heuristique, un niveau de risque de 1 - Bon (vert) à 9 - Risqué (rouge) est attribué aux objets. Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations d'ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui doivent faire l'objet d'un examen plus approfondi en cas de comportement étrange.

Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec une signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

Qu'est-ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth offre une détection efficace des rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utilisateur risque une perte ou un vol de données. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

Pourquoi y a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsqu'il tente d'identifier la signature numérique d'un fichier exécutable, ESET SysInspector recherche d'abord une signature numérique intégrée au fichier. Si une signature numérique est détectée, le fichier est validaté à l'aide de ces informations. En revanche, si aucune signature numérique n'est détectée, ESI lance la recherche du fichier CAT correspondant (Catalogue de sécurité - *%systemroot%\system32\catroot*) qui contient les informations relatives au fichier exécutable traité. Si le fichier CAT pertinent est trouvé, la signature numérique du fichier CAT est appliquée dans la procédure de validation du fichier exécutable.

Voilà pourquoi des fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 comprend l'application HyperTerminal qui se trouve dans *C:\Program Files\Windows NT*. Le fichier exécutable principal de l'application n'a pas de signature numérique, mais ESET SysInspector l'indique comme étant un fichier signé par Microsoft. Ceci s'explique par une référence dans *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* qui pointe vers *C:\Program Files\Windows NT\hypertrm.exe* (le fichier exécutable principal de l'application HyperTerminal) et *sp4.cat* qui possède une signature numérique de Microsoft.

4.7.8 ESET SysRescue Live

ESET SysRescue Live est un utilitaire qui permet de créer un disque amorçable contenant une des solutions ESET Security : ESET NOD32 Antivirus, ESET Smart Security ou l'un des produits orientés serveur. Le principal avantage d'ESET SysRescue Live réside dans le fait que la solution ESET Security est exécutée indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et au système de fichiers. Il est par conséquent possible de supprimer les infiltrations qui ne pourraient normalement pas être supprimées, par exemple lorsque le système d'exploitation est en cours d'exécution.

4.7.9 Planificateur

Le planificateur gère et lance les tâches planifiées avec des configurations et des propriétés prédéfinies. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils à utiliser pendant l'exécution de la tâche.

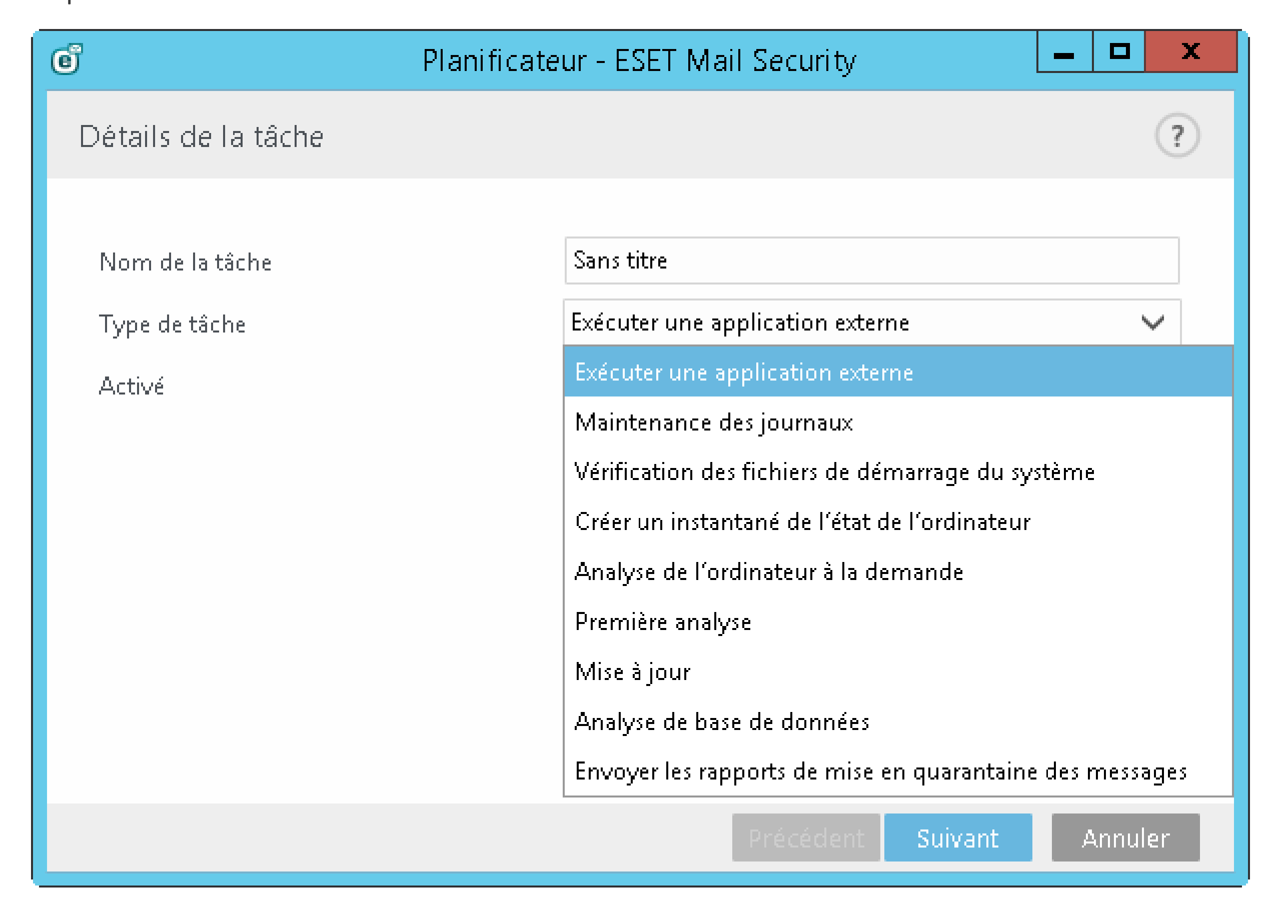
Le planificateur est accessible depuis la fenêtre principale de ESET Mail Security, dans **Outils** > **Planificateur**. Le **planificateur** contient la liste de toutes les tâches planifiées, des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.

Il sert à planifier les tâches suivantes : la mise à jour de la base des signatures de virus, l'analyse, le contrôle des fichiers de démarrage du système et la maintenance des journaux. Vous pouvez ajouter ou supprimer des tâches dans la fenêtre principale du planificateur (cliquez sur **Ajouter une tâche** ou **Supprimer** dans la partie inférieure). Cliquez avec le bouton droit dans la fenêtre du planificateur pour effectuer les actions suivantes : afficher des informations détaillées, exécuter la tâche immédiatement, ajouter une nouvelle tâche ou supprimer une tâche existante. Utilisez les cases à cocher au début de chaque entrée pour activer/désactiver les tâches.

Par défaut, les tâches planifiées suivantes sont affichées dans le **planificateur** :

- **Maintenance des journaux**
- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion d'accès à distance**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)
- **Vérification automatique des fichiers de démarrage** (après la réussite de la mise à jour de la base des signatures de virus)
- **Première analyse automatique**

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier**. Vous pouvez également sélectionner la tâche à modifier et cliquer sur **Modifier**.



Ajout d'une nouvelle tâche

1. Cliquez sur **Ajouter une tâche** dans la partie inférieure de la fenêtre.
2. Entrez le nom de la tâche.

3. Sélectionnez la tâche souhaitée dans le menu déroulant :

- **Exécuter une application externe** - Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** - Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Analyse de l'ordinateur** - Crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** : effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Première analyse** - Par défaut, 20 minutes après une installation ou un redémarrage, une analyse de l'ordinateur sera effectuée en tant que tâche de faible priorité.
- **Mise à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules de l'application.

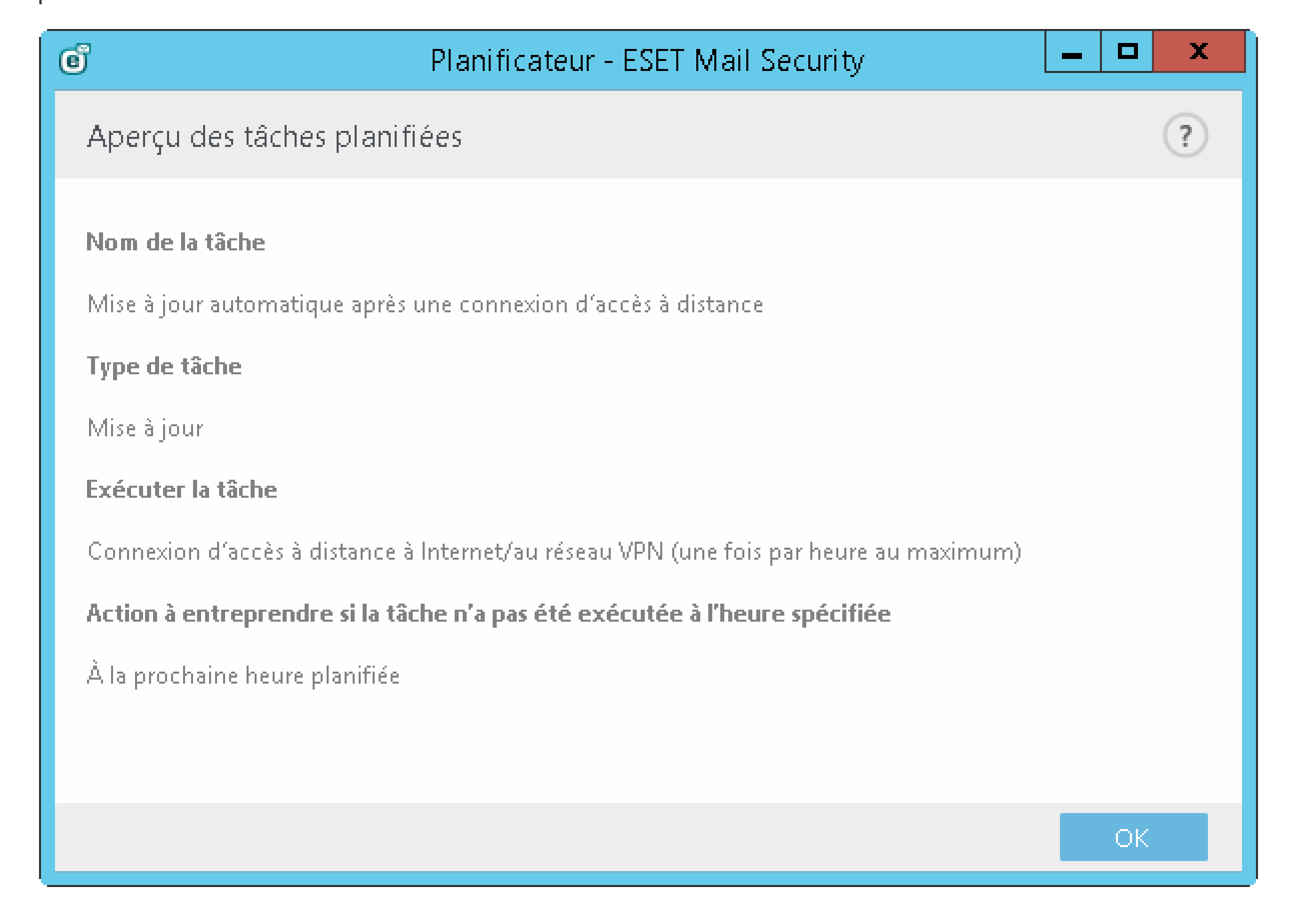
4. Cliquez sur **Activé** si vous souhaitez activer la tâche (vous pouvez le faire ultérieurement en activant/désactivant la case à cocher correspondante dans la liste des tâches planifiées). Cliquez ensuite sur **Suivant** et sélectionnez une des options de planification :

- **Une fois** - La tâche est exécutée à la date et à l'heure prédéfinies.
- **Plusieurs fois** - La tâche est exécutée aux intervalles indiqués.
- **Quotidiennement** - La tâche est exécutée tous les jours à l'heure définie.
- **Chaque semaine** - La tâche est exécutée à l'heure et au jour prédéfinis.
- **Déclenchée par un événement** - La tâche est exécutée après un événement particulier.

5. Sélectionnez **Ignorer la tâche en cas d'alimentation par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Cette tâche est exécutée à l'heure et au jour spécifiées dans les champs **Exécution de tâche**. Si la tâche n'a pas pu être exécutée au moment défini, vous pouvez désigner le moment auquel elle doit être réexécutée :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée** (l'intervalle peut être spécifié dans la zone de liste déroulante **Durée écoulée depuis la dernière exécution**.)

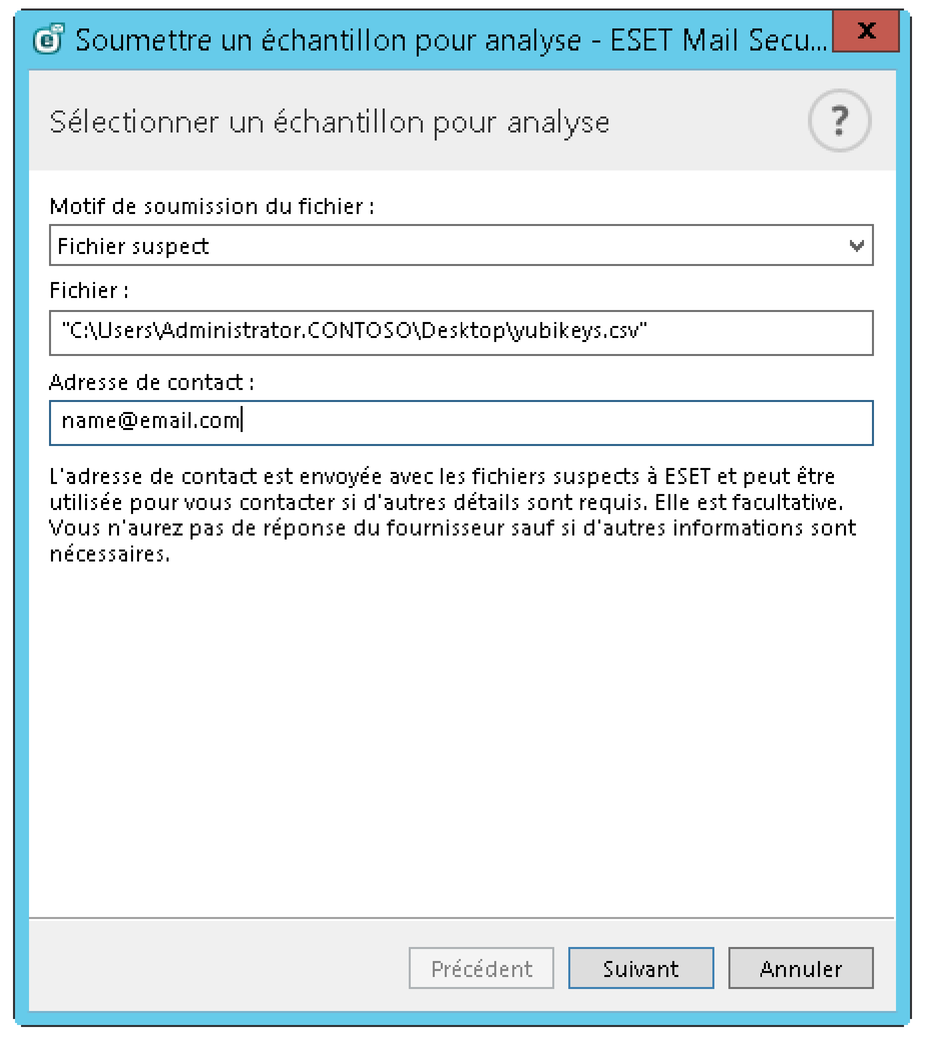
Cliquez avec le bouton droit sur une tâche et cliquez sur **Afficher les détails des tâches** dans le menu contextuel pour afficher les informations concernant la tâche.



4.7.10 Soumettre les échantillons pour analyse

La boîte de dialogue de soumission d'échantillons permet d'envoyer un fichier ou un site à ESET pour analyse ; elle est accessible dans **Outils** > **Soumettre un échantillon pour analyse**. Si vous trouvez sur votre ordinateur un fichier dont le comportement est suspect, vous pouvez le soumettre au laboratoire de recherche sur les menaces d'ESET pour analyse. Si le fichier s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour.

Vous pouvez également soumettre le fichier par e-mail. Pour ce faire, compressez le ou les fichiers à l'aide de WinRAR ou de WinZip, protégez l'archive à l'aide du mot de passe « infected » et envoyez-la à samples@eset.com. Veillez à utiliser un objet descriptif et indiquez le plus d'informations possible sur le fichier (notez par exemple le site Internet à partir duquel vous l'avez téléchargé).



REMARQUE : avant de soumettre un échantillon à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :

- Le fichier ou le site Web n'est pas du tout détecté.
- Le fichier ou le site Web est détecté à tort comme une menace.

Vous ne recevrez pas de réponse, excepté si des informations complémentaires sont nécessaires à l'analyse.

Sélectionnez dans le menu déroulant **Motif de soumission de l'échantillon** la description correspondant le mieux à votre message :

- **Fichier suspect**
- **Site suspect** (site Web infecté par un logiciel malveillant quelconque)
- **Fichier faux positif** (fichier détecté à tort comme infecté)
- **Site faux positif**
- **Autre**

Fichier/Site : le chemin d'accès au fichier ou au site Web que vous souhaitez soumettre.

Adresse de contact : l'adresse de contact est envoyée à ESET avec les fichiers suspects. Elle pourra servir à vous contacter si des informations complémentaires sont nécessaires à l'analyse. La spécification d'une adresse de contact est facultative. Vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires sont nécessaires à l'analyse. En effet, nos serveurs reçoivent chaque jour des dizaines de milliers de fichiers, ce qui ne permet pas de répondre à tous les envois.

4.7.10.1 Fichier suspect

Signes et symptômes observés d'infection par logiciel malveillant : saisissez une description du comportement du fichier suspect que vous avez observé sur votre ordinateur.

Origine du fichier (adresse URL ou fournisseur) : indiquez l'origine du fichier (sa source) et comment vous l'avez trouvé.

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront le processus d'identification du fichier suspect.

i **REMARQUE :** le premier paramètre (**Signes et symptômes observés d'infection par logiciel malveillant**) est obligatoire. Les autres informations faciliteront la tâche de nos laboratoires lors du processus d'identification des échantillons.

4.7.10.2 Site suspect

Dans le menu déroulant **Pourquoi ce site est-il suspect ?**, sélectionnez l'une des options suivantes :

- **Infecté** : un site Web qui contient des virus ou d'autres logiciels malveillants diffusés par diverses méthodes.
- **Hameçonnage** : souvent utilisé pour accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc. Pour en savoir plus sur ce type d'attaque, consultez le glossaire.
- **Scam** : un site d'escroquerie ou frauduleux.
- Sélectionnez **Autre** si les options ci-dessus ne correspondent pas au site que vous allez soumettre.

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront l'analyse du site Web suspect.

4.7.10.3 Fichier faux positif

Nous vous invitons à soumettre les fichiers qui sont signalés comme infectés alors qu'ils ne le sont pas, afin d'améliorer notre moteur antivirus et antispyware et contribuer à la protection des autres utilisateurs. Les faux positifs (FP) peuvent se produire lorsque le motif d'un fichier correspond à celui figurant dans une base des signatures de virus.

Nom et version de l'application : titre et version du programme (par exemple : numéro, alias et nom de code).

Origine du fichier (adresse URL ou fournisseur) : indiquez l'origine du fichier (sa source) et comment vous l'avez trouvé.

Objectif des applications : description générale, type (navigateur, lecteur multimédia, etc.) et fonctionnalité de l'application.

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront le traitement du fichier suspect.

i **REMARQUE :** les trois premiers paramètres sont nécessaires pour identifier les applications légitimes et les distinguer des codes malveillants. En fournissant des informations supplémentaires, vous facilitez l'identification et le traitement des échantillons par nos laboratoires.

4.7.10.4 Site faux positif

Nous vous recommandons de soumettre les sites faussement détectés comme infectés ou signalés à tort comme scam ou hameçonnage. Les faux positifs (FP) peuvent se produire lorsque le motif d'un fichier correspond à celui figurant dans une base des signatures de virus. Veuillez soumettre ce site Web afin d'améliorer notre moteur antivirus et antihameçonnage, et contribuer à la protection des autres utilisateurs.

Notes et autres informations - Saisissez éventuellement d'autres informations ou une description qui faciliteront le traitement du fichier suspect.

4.7.10.5 Autre

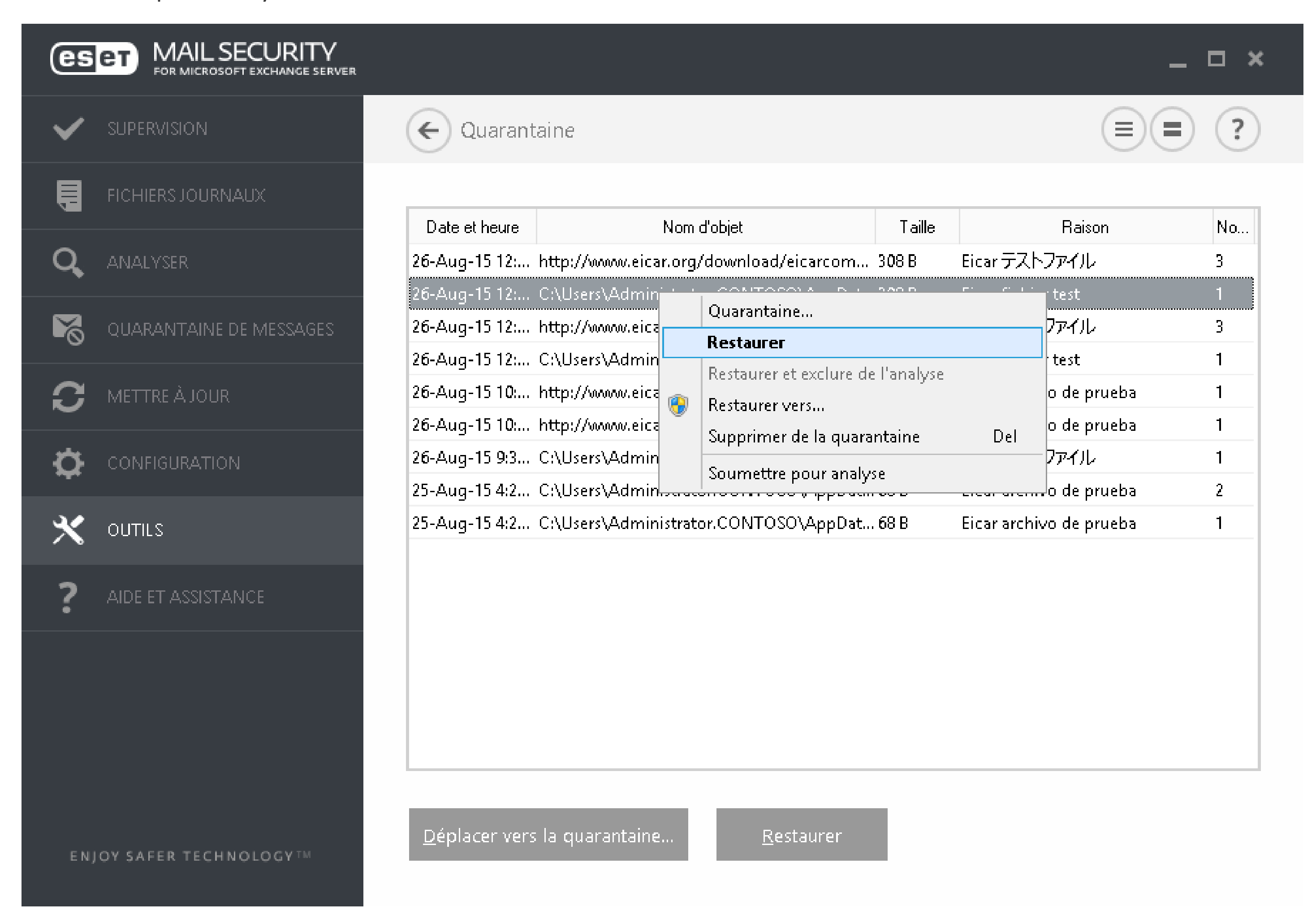
Utilisez ce formulaire si le fichier ne peut pas être classé par catégorie en tant que **fichier suspect** ou **faux positif**.

Motif de soumission du fichier - Décrivez en détail le motif d'envoi du fichier.

4.7.11 Quarantaine

La principale fonction de la quarantaine est de stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Mail Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte, mais n'a pas été détecté par l'analyseur antivirus. Les fichiers en quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple, objet ajouté par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple).

Mise en quarantaine de fichiers

ESET Mail Security met automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désactivé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine.** Les fichiers d'origine sont supprimés de leur emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Quarantaine**.

Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. L'option **Restaurer** est disponible dans le menu contextuel accessible en cliquant avec le bouton droit sur le fichier dans le fenêtre Quarantaine. Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est également disponible. Pour en savoir plus sur ce type d'application, consultez le glossaire. Le menu contextuel propose également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

REMARQUE : si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service client d'ESET.

Soumission de fichiers mis en quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

4.8 Aide et assistance

ESET Mail Security contient des outils de dépannage et des informations d'assistance qui vous aideront à résoudre les problèmes que vous pouvez rencontrer.

Aide

- **Consulter la base de connaissances ESET** - La base de connaissances ESET contient des réponses aux questions les plus fréquentes et les solutions recommandées pour résoudre divers problèmes. Régulièrement mise à jour par les spécialistes techniques d'ESET, la base de connaissances est l'outil le plus puissant pour résoudre différents types de problèmes.
- **Ouvrir l'aide** - Cliquez sur ce lien pour lancer les pages d'aide ESET Mail Security.
- **Trouver une solution rapide** : cette option permet de trouver les solutions aux problèmes les plus fréquents. Nous vous recommandons de lire cette section avant de contacter le service d'assistance technique.

Service client

- **Envoyer une demande d'assistance** - Si vous ne trouvez pas de réponse à votre problème, vous pouvez également utiliser le formulaire situé sur le site Web d'ESET pour prendre rapidement contact avec notre service client.

Outils d'assistance

Encyclopédie des menaces - Permet d'accéder à l'encyclopédie des menaces ESET, qui contient des informations sur les dangers et les symptômes de différents types d'infiltration.

Historique de la base des signatures de virus - Mène à ESET Virus radar, qui contient des informations sur les versions de la base des signatures de virus ESET.

Nettoyeur spécialisé - Ce nettoyeur identifie et supprime automatiquement les infections courantes par logiciels malveillants. Pour obtenir plus d'informations, consultez cet article de la base de connaissances ESET.

Informations sur le produit et la licence

- **À propos de ESET Mail Security** - Affiche des informations sur votre copie de ESET Mail Security.
- Gérer la licence - Cliquez sur cette option pour ouvrir la fenêtre Activation du produit. Sélectionnez l'une des méthodes disponibles pour activer ESET Mail Security. Pour plus d'informations, reportez-vous à la section Comment activer ESET Mail Security.

4.8.1 Procédures

Ce chapitre couvre les questions et les problèmes les plus fréquents. Cliquez sur l'intitulé d'une rubrique pour apprendre comment résoudre le problème :

Comment mettre à jour ESET Mail Security

Comment activer ESET Mail Security

Comment programmer une tâche d'analyse (toutes les 24 heures)

Comment éliminer un virus de mon serveur

Fonctionnement des exclusions automatiques

Si votre problème n'est pas couvert dans la liste des pages d'aide ci-dessus, essayez d'effectuer une recherche par mot-clé ou entrez un ou plusieurs mots décrivant votre problème et lancez la recherche dans les pages d'aide d'ESET Mail Security.

Si vous ne trouvez pas la solution à votre problème/question dans les pages d'aide, vous pouvez consulter notre base de connaissances en ligne qui est régulièrement mise à jour.

Au besoin, vous pouvez contacter directement notre centre d'assistance technique en ligne pour soumettre vos questions ou problèmes. Le formulaire de contact est disponible dans l'onglet Aide et support de votre programme ESET.

4.8.1.1 Comment mettre à jour ESET Mail Security

La mise à jour d'ESET Mail Security peut être effectuée manuellement ou automatiquement. Pour déclencher la mise à jour, cliquez sur **Mettre à jour la base des signatures de virus**. Il se trouve dans la section **Mise à jour du programme**.

Les paramètres d'installation par défaut créent une tâche de mise à jour automatique qui s'exécute chaque heure. Pour changer l'intervalle, accédez au **Planificateur** (pour plus d'informations sur le Planificateur, cliquez ici).

4.8.1.2 Comment activer ESET Mail Security

Une fois l'installation terminée, vous êtes invité à activer le produit.

Plusieurs méthodes permettent d'activer le produit. Certains scénarios d'activation proposés dans la fenêtre d'activation peuvent varier en fonction du pays et selon le mode de distribution (CD/DVD, page Web ESET, etc.).

Pour activer votre copie d'ESET Mail Security directement à partir du programme, cliquez sur l'icône dans la partie système de la barre des tâches, puis sélectionnez **Activer la licence du produit** dans le menu. Vous pouvez également activer le produit dans le menu principal sous **Aide et assistance** > **Activer la licence** ou **État de la protection** > **Activer la licence du produit**.

Pour activer ESET Mail Security, vous pouvez utiliser l'une des méthodes suivantes :

- **Clé de licence** : chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le propriétaire de la licence et à activer la licence.
- **Compte Administrateur Sécurité** : compte créé sur le portail ESET License Administrator à l'aide d'informations d'identification (adresse électronique + mot de passe). Cette méthode permet de gérer plusieurs licences à partir d'un seul emplacement.
- **Fichier de licence hors ligne** : fichier généré automatiquement qui est transféré au produit ESET afin de fournir

des informations de licence. Ce fichier de licence hors ligne est généré à partir du portail des licences. Il est utilisé dans les environnements dans lesquelles l'application ne peut pas se connecter à l'autorité de certification.

Cliquez sur **Activer ultérieurement** avec ESET Remote Administrator si votre ordinateur est membre d'un réseau géré et si l'administrateur effectue l'activation à distance via ESET Remote Administrator. Vous pouvez également utiliser cette option si vous souhaitez activer ce client ultérieurement.

Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Gérer la licence** pour gérer les informations de licence à tout moment. L'ID de licence publique s'affiche ; il sert à identifier votre produit et votre licence auprès d'ESET. Le nom d'utilisateur sous lequel l'ordinateur est enregistré auprès du système de gestion des licences est stocké dans la section **À propos**. Il est visible lorsque vous cliquez avec le bouton droit sur l'icône dans la partie système de la barre des tâches.

REMARQUE : ESET Remote Administrator peut activer des ordinateurs clients en silence à l'aide des licences fournies par l'administrateur.

4.8.1.3 Comment créer une tâche dans le Planificateur

Pour créer une tâche dans **Outils** > **Planificateur**, cliquez sur **Ajouter une tâche** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe** - Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** - Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Créer un rapport de l'état de l'ordinateur** : crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** : effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Première analyse** : par défaut, 20 minutes après une installation ou un redémarrage, une analyse de l'ordinateur sera effectuée en tant que tâche de faible priorité.
- **Mise à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules de l'application.

La tâche planifiée la plus fréquente étant la **mise à jour**, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour :

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mise à jour**. Saisissez le nom de la tâche dans le champ **Nom de la tâche**, puis cliquez sur **Suivant**. Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidienne**, **Hebdomadaire** et **Déclenchée par un événement.** Sélectionnez **Ignorer la tâche en cas d'alimentation par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Cette tâche est exécutée à l'heure et au jour spécifiées dans les champs **Exécution de tâche**. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les options disponibles sont les suivantes :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée** (l'intervalle peut être spécifié dans la zone de liste déroulante Durée écoulée depuis la dernière exécution)

À l'étape suivante, une fenêtre de synthèse apparaît. Elle contient des informations sur la tâche planifiée actuelle. Lorsque vous avez terminé vos modifications, cliquez sur **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. Vous pouvez y définir le profil principal et le profil secondaire. Le profil secondaire est utilisé si la tâche ne peut pas être terminée à l'aide du profil principal. Cliquez sur **Terminer** pour ajouter la nouvelle tâche planifiée à la liste des tâches actuellement planifiées.

4.8.1.4 Comment programmer une tâche d'analyse (toutes les 24 heures)

Pour planifier une tâche régulière, accédez à **ESET Mail Security** > **Outils** > **Planificateur**. Vous trouverez ci-dessous un guide abrégé indiquant comment planifier une tâche qui analyse les disques locaux toutes les 24 heures.

Pour programmer une tâche d'analyse :

1. Cliquez sur **Ajouter** dans l'écran principal du planificateur.
2. Sélectionnez **Analyse de l'ordinateur à la demande** dans le menu déroulant.
3. Saisissez un nom pour la tâche et sélectionnez **Plusieurs fois**.
4. Choisissez de lancer la tâche toutes les 24 heures (1 440 minutes).
5. Sélectionnez une action à effectuer en cas de non-exécution de la tâche planifiée, quel qu'en soit le motif.
6. Passez en revue le résumé de la tâche planifiée, puis cliquez sur **Terminer**.
7. Dans le menu déroulant **Cibles**, sélectionnez Disques locaux.
8. Cliquez sur **Terminer** pour appliquer la tâche.

4.8.1.5 Comment éliminer un virus de votre serveur

Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, par exemple), nous recommandons d'effectuer les opérations suivantes :

1. Dans la fenêtre principale ESET Mail Security, cliquez sur **Analyse de l'ordinateur**.

2. Cliquez sur **Analyse intelligente** pour démarrer l'analyse de votre système.

3. Une fois l'analyse terminée, consultez le journal pour s'informer sur le nombre de fichiers analysés, infectés et nettoyés.

4. Si vous ne souhaitez analyser qu'une certaine partie de votre disque, choisissez **Analyse personnalisée** et sélectionnez les cibles à analyser.

4.8.2 Envoyer une demande d'assistance

Pour offrir l'assistance adéquate le plus rapidement possible, ESET requiert des informations sur la configuration de ESET Mail Security, sur le système et les processus en cours (fichier journal ESET SysInspector), ainsi que les données du Registre. ESET utilise ces données uniquement pour fournir une assistance technique au client.

Lorsque vous envoyez le formulaire Web, les données de configuration de votre système sont également envoyées à ESET. Sélectionnez **Toujours envoyer ces informations** si vous souhaitez mémoriser cette action pour ce processus. Pour soumettre le formulaire sans envoyer de données, cliquez sur **Ne pas envoyer les données**. Vous pouvez ainsi contacter le service client ESET à l'aide du formulaire d'assistance en ligne.

Ce paramètre peut être également configuré dans **Configuration avancée** > **Outils** > **Diagnostics** > **Service client**.

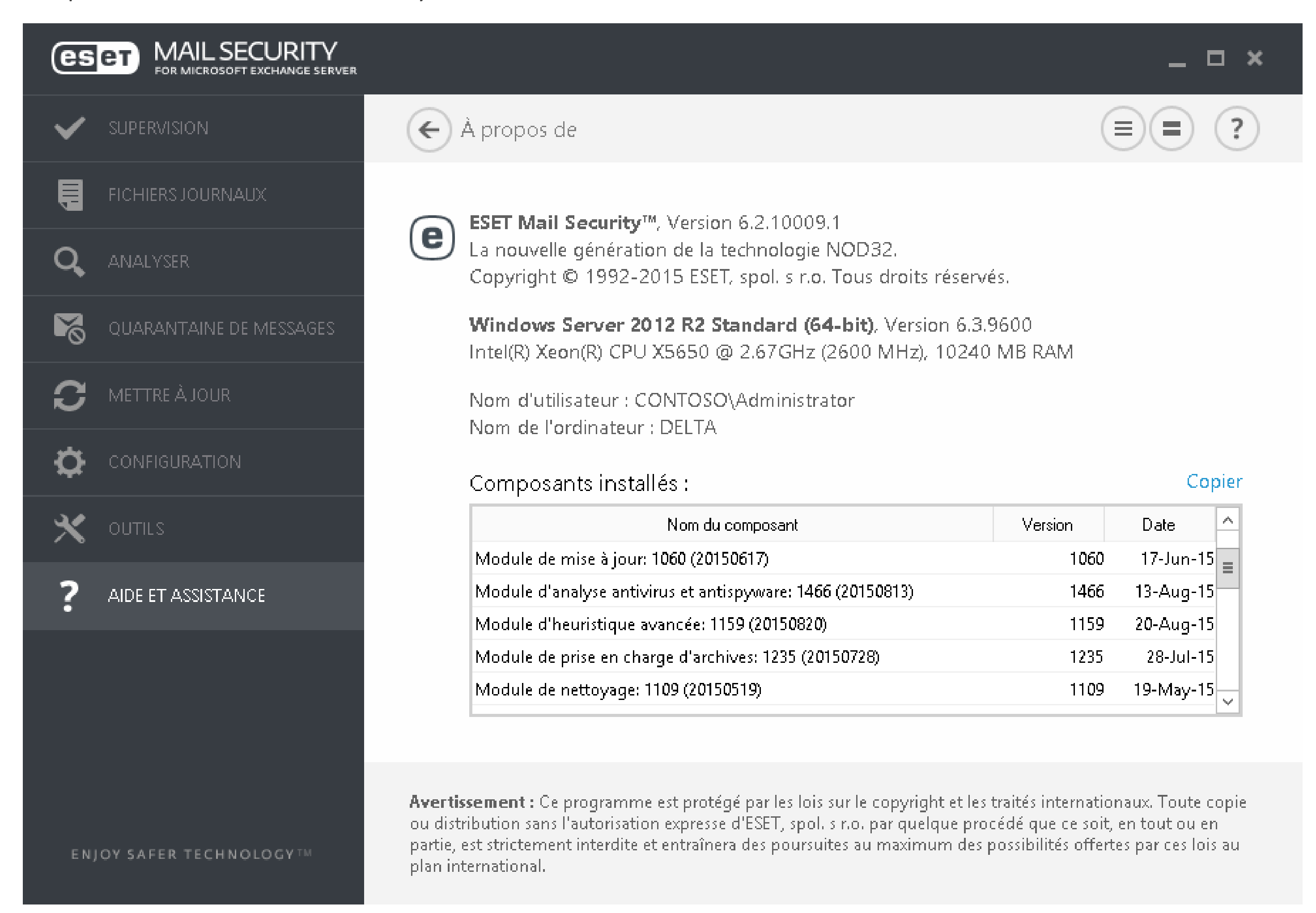
i **REMARQUE**: si vous avez décidé d'envoyer les données système, vous devez remplir le formulaire Web et l'envoyer. Sinon, votre ticket n'est pas créé et vos données système sont perdues.

4.8.3 ESET Outil de nettoyage spécialisé

L'outil de nettoyage spécialisé ESET est un outil de suppression des infections courantes par logiciels malveillants tels que Conficker, Sirefef ou Necurs. Pour plus d'informations, consultez cet article de la base de connaissances ESET.

4.8.4 À propos d'ESET Mail Security

Cette fenêtre comporte des informations détaillées sur la version d'ESET Mail Security installée, et répertorie les modules du programme installés. La partie supérieure de la fenêtre comporte des informations sur le système d'exploitation et les ressources du système.



Vous pouvez copier les informations sur les modules (**Composants installés**) dans le Presse-papiers en cliquant sur **Copier**. Ce procédé peut être utile pour la résolution des problèmes ou lorsque vous contactez l'assistance technique.

4.8.5 Activation du produit

Une fois l'installation terminée, vous êtes invité à activer le produit.

Plusieurs méthodes permettent d'activer le produit. Certains scénarios d'activation proposés dans la fenêtre d'activation peuvent varier en fonction du pays et selon le mode de distribution (CD/DVD, page Web ESET, etc.).

Pour activer votre copie d'ESET Mail Security directement à partir du programme, cliquez sur l'icône dans la partie système de la barre des tâches, puis sélectionnez **Activer la licence du produit** dans le menu. Vous pouvez également activer le produit dans le menu principal sous **Aide et assistance** > **Activer la licence** ou **État de la protection** > **Activer la licence du produit**.

Pour activer ESET Mail Security, vous pouvez utiliser l'une des méthodes suivantes :

- **Clé de licence** : chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le propriétaire de la licence et à activer la licence.
- **Compte Administrateur Sécurité** : compte créé sur le portail ESET License Administrator à l'aide d'informations d'identification (adresse électronique + mot de passe). Cette méthode permet de gérer plusieurs licences à partir d'un seul emplacement.
- **Fichier de licence hors ligne** : fichier généré automatiquement qui est transféré au produit ESET afin de fournir des informations de licence. Ce fichier de licence hors ligne est généré à partir du portail des licences. Il est utilisé dans les environnements dans lesquelles l'application ne peut pas se connecter à l'autorité de certification.

Cliquez sur **Activer ultérieurement** avec ESET Remote Administrator si votre ordinateur est membre d'un réseau géré et si l'administrateur effectue l'activation à distance via ESET Remote Administrator. Vous pouvez également utiliser cette option si vous souhaitez activer ce client ultérieurement.

Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Gérer la licence** pour gérer les informations de licence à tout moment. L'ID de licence publique s'affiche ; il sert à identifier votre produit et votre licence auprès d'ESET. Le nom d'utilisateur sous lequel l'ordinateur est enregistré auprès du système de gestion des licences est stocké dans la section **À propos**. Il est visible lorsque vous cliquez avec le bouton droit sur l'icône dans la partie système de la barre des tâches.

REMARQUE : ESET Remote Administrator peut activer des ordinateurs clients en silence à l'aide des licences fournies par l'administrateur.

4.8.5.1 Enregistrement

Veuillez enregistrer votre licence en renseignant les champs contenus dans le formulaire d'enregistrement, puis en cliquant sur **Continuer**. Les champs signalés comme obligatoires sont requis. Ces informations seront utilisées uniquement pour les questions liées à votre licence ESET.

4.8.5.2 Activation de Security Admin

Le compte Security Admin est un compte créé sur le portail des licences à l'aide de vos **adresse électronique** et **mot de passe**. Il peut voir toutes les autorisations des sièges. Un compte Security Admin permet de gérer plusieurs licences. Si vous n'en avez pas, cliquez sur **Créer un compte** pour être redirigé vers la page Web d'ESET License Administrator dans laquelle vous pouvez vous enregistrer à l'aide de vos informations d'identification.

Si vous avez oublié votre mot de passe, cliquez sur **Mot de passe oublié ?** pour être redirigé vers le portail ESET Business. Saisissez votre adresse électronique et cliquez sur **Envoyer**. Vous recevrez ensuite un message contenant des instructions pour réinitialiser votre mot de passe.

REMARQUE : pour plus d'informations sur l'utilisation d'ESET License Administrator, reportez-vous au guide de l'utilisateur ESET License Administrator.

4.8.5.3 Échec de l'activation

L'activation d'ESET Mail Security a échoué. Vérifiez que vous avez saisi la **clé de licence** correcte ou que vous avez associé une **licence hors ligne**. Si vous disposez d'une **licence hors ligne** différente, saisissez-la de nouveau. Pour vérifier la clé de licence que vous avez saisie, cliquez sur **revérifier la clé de licence** ou sur **acheter une nouvelle licence** afin d'être redirigé vers notre page Web dans laquelle vous pouvez acheter une nouvelle licence.

4.8.5.4 Licence

Si vous sélectionnez l'option d'activation Security Admin, vous êtes invité à sélectionner une licence associée à votre compte qui sera utilisée pour ESET Mail Security. Cliquez sur **Activer** pour continuer.

4.8.5.5 Progression de l'activation

ESET Mail Security procède maintenant à l'activation. Veuillez patienter. Cette opération peut prendre quelques minutes.

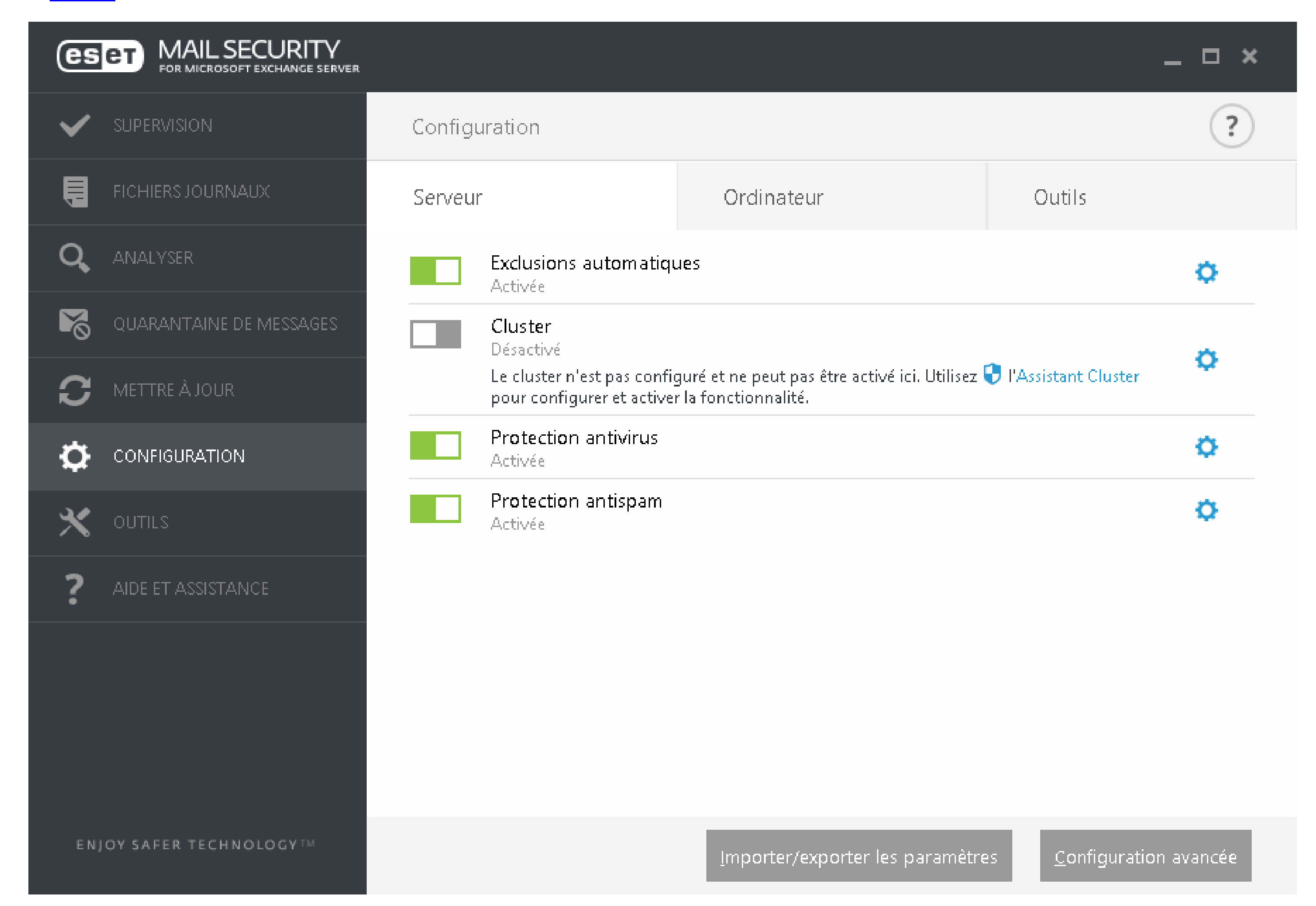
4.8.5.6 Activation réussie

L'activation a été effectuée, et ESET Mail Security est désormais activé. À partir de maintenant, ESET Mail Security recevra des mises à jour régulières pour identifier les menaces les plus récentes et protéger votre ordinateur. Cliquez sur **Terminé** pour terminer l'activation du produit.

5. Utilisation d'ESET Mail Security

Le menu **Configuration** contient les sections suivantes auxquelles vous pouvez accéder grâce à des onglets :

- Serveur
- Ordinateur
- Outils



Pour désactiver temporairement un module, cliquez sur le bouton bascule vert situé en regard. Notez que cette opération peut diminuer le niveau de protection de l'ordinateur.
Pour réactiver la protection d'un composant de sécurité désactivé, cliquez sur le bouton bascule rouge .
Pour accéder aux paramètres détaillés d'un composant de sécurité spécifique, cliquez sur l'engrenage .

Cliquez sur **Configuration avancée** ou appuyez sur **F5** pour accéder à des paramètres et des options supplémentaires.

D'autres options sont disponibles au bas de la fenêtre de configuration. Pour charger les paramètres de configuration à l'aide d'un fichier de configuration *.xml* ou pour enregistrer les paramètres de configuration actuels dans un fichier de configuration, utilisez l'option **Importer/exporter les paramètres**. Pour plus d'informations, consultez la section Importer/exporter les paramètres.

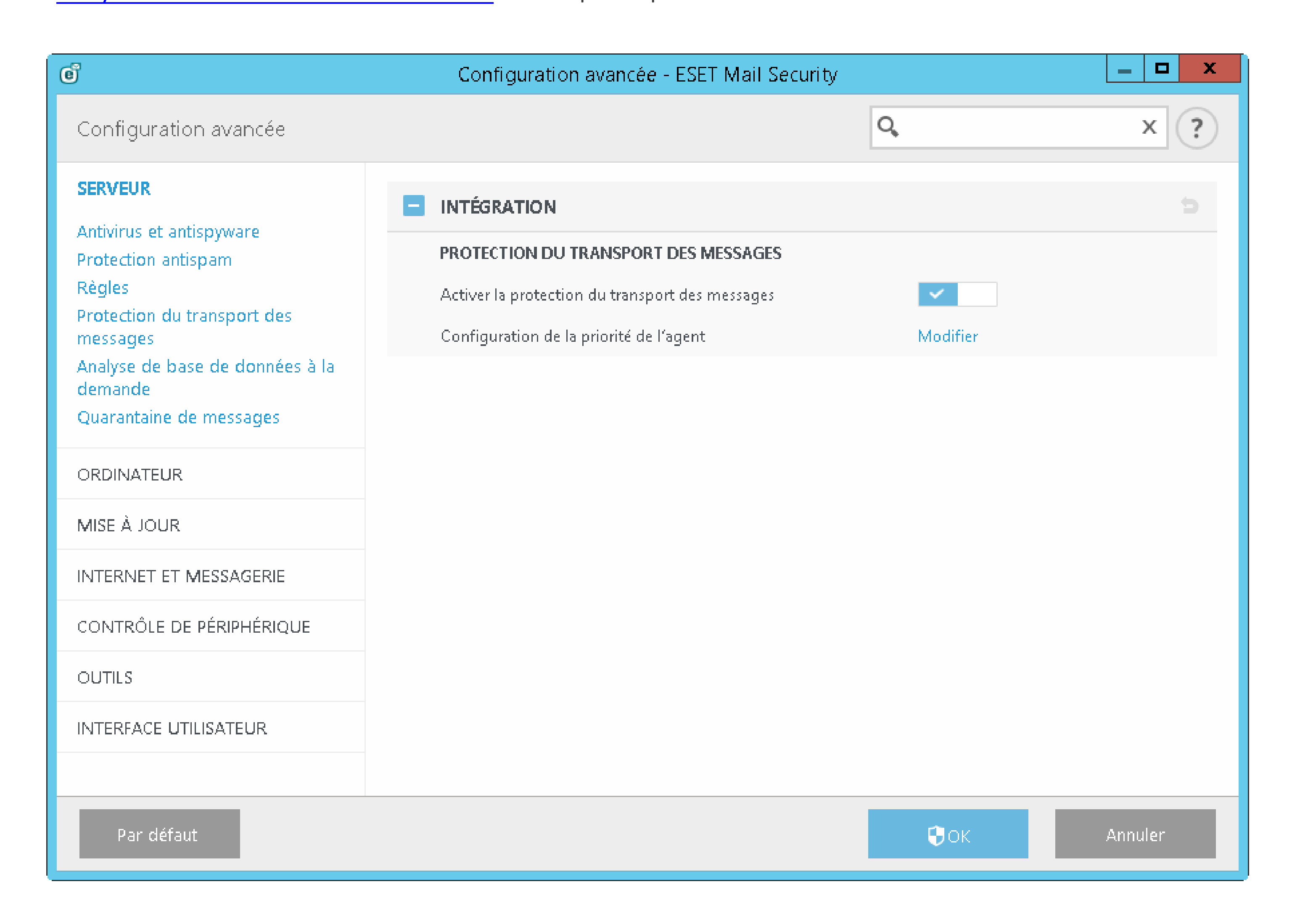
5.1 Serveur

ESET Mail Security offre à votre serveur Microsoft Exchange Server une excellente protection grâce aux fonctionnalités suivantes :

- Antivirus et antispyware
- Protection antispam
- Règles
- Protection du transport des messages (Exchange Server 2007, 2010, 2013)
- Protection de la base de données des boîtes aux lettres (Exchange Server 2003, 2007, 2010)
- Analyse de base de données à la demande (Exchange Server 2007, 2010, 2013)
- Quarantaine (paramètres du type de quarantaine de messages)

Cette section de la configuration avancée vous permet d'activer ou de désactiver la protection de la base de données des boîtes aux lettres et la protection du transport des messages et de modifier la priorité de l'Agent.

REMARQUE : si vous exécutez Microsoft Exchange Server 2007 ou 2010 vous pouvez choisir entre la protection de la base de données de boîtes aux lettres et une analyse de base de données à la demande. Sachez toutefois qu'une seule de ces deux protections peut être active à la fois. Si vous choisissez d'utiliser l'analyse de base de données à la demande, vous devez désactiver l'intégration de la protection de la base de données de boîtes aux lettres. Sinon, l'analyse de base de données à la demande ne sera pas disponible.



5.1.1 Configuration de la priorité des agents

Dans le menu **Configuration de la priorité des agents**, vous pouvez définir la priorité selon laquelle les Agents ESET Mail Security deviennent actifs après le démarrage de Microsoft Exchange Server. Une valeur numérique définit la priorité. Plus la valeur est faible, plus la priorité est élevée. Cette configuration s'applique à Microsoft Exchange 2003.

Cliquez sur le bouton **Modifier** pour accéder à la configuration de la priorité des agents. Vous pouvez définir la priorité d'activation des Agents ESET Mail Security après le démarrage de Microsoft Exchange Server.

- **Modifier** : définissez manuellement une valeur pour modifier la priorité de l'Agent sélectionné.
- **Monter** : augmente la priorité de l'Agent sélectionné par son déplacement vers le haut dans la liste des Agents.
- **Descendre** : diminue la priorité de l'Agent sélectionné par son déplacement vers le bas dans la liste des Agents.

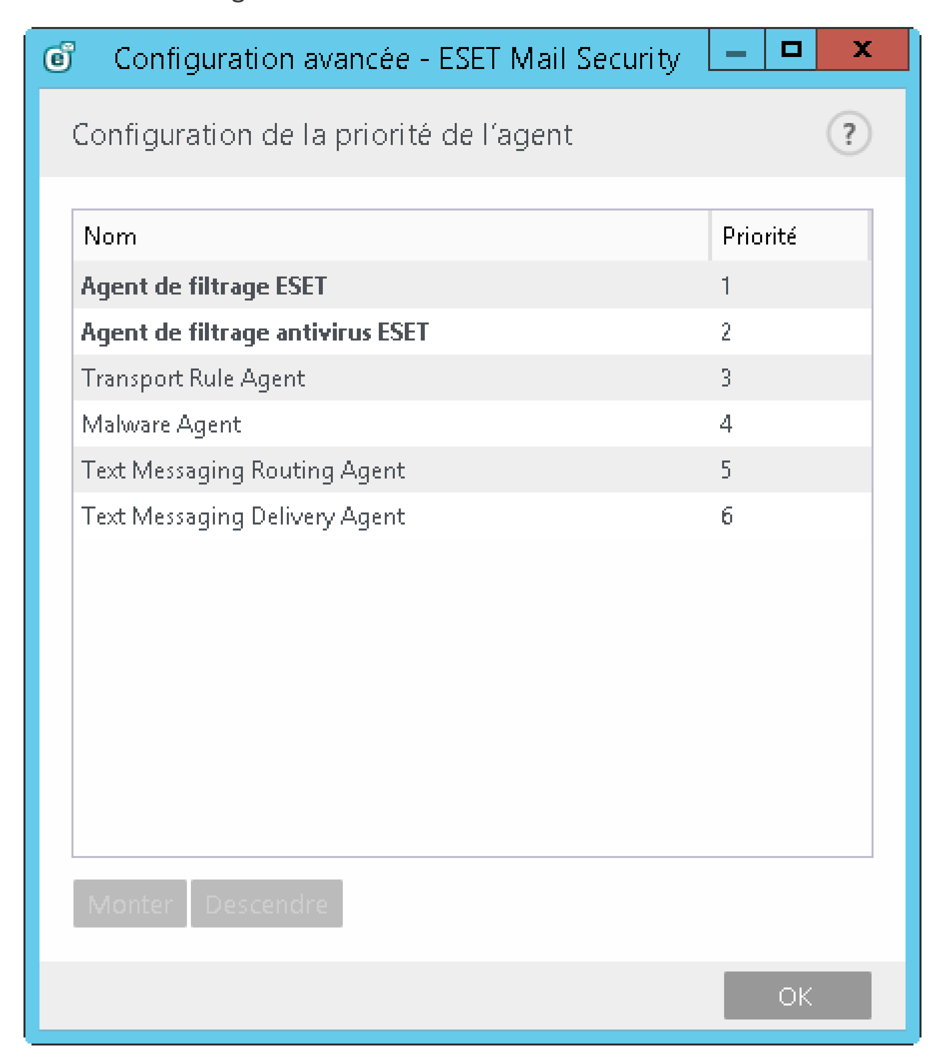
Avec Microsoft Exchange Server 2003, vous pouvez spécifier la priorité des Agents indépendamment à l'aide d'onglets pour la fin des données et le destinataire.

5.1.1.1 Modifier la priorité

Si vous exécutez Microsoft Exchange Server 2003, vous pouvez définir manuellement une valeur pour modifier la **priorité de l'agent de transport**. Modifiez la valeur dans le champ de texte ou utilisez les flèches Haut et Bas pour modifier la priorité. Plus la valeur est faible, plus la priorité est élevée.

5.1.2 Configuration de la priorité des agents

Dans le menu **Configuration de la priorité des agents**, vous pouvez définir la priorité selon laquelle les Agents ESET Mail Security deviennent actifs après le démarrage de Microsoft Exchange Server. Cette configuration s'applique à Microsoft Exchange 2007 et version ultérieure.



- **Monter** : augmente la priorité de l'Agent sélectionné par son déplacement vers le haut dans la liste des Agents.
- **Descendre** : diminue la priorité de l'Agent sélectionné par son déplacement vers le bas dans la liste des Agents.

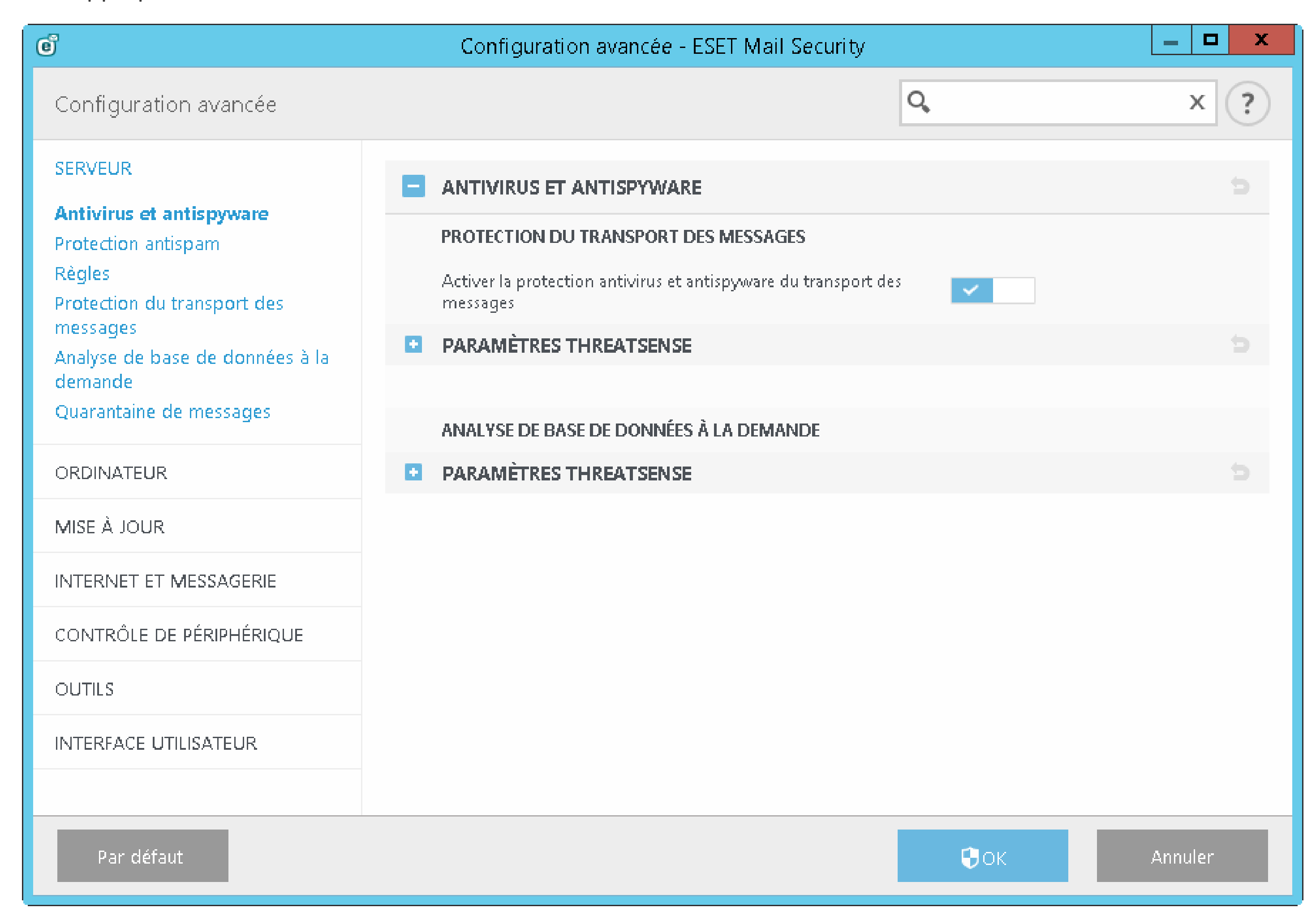
5.1.3 Antivirus et antispyware

Dans cette section, vous pouvez configurer les options **Antivirus et antispyware** pour votre serveur de messagerie.

Important : la protection du transport des messages est assurée par l'agent de transport et est uniquement disponible pour Microsoft Exchange Server 2007 ou version ultérieure. Votre serveur Exchange Server doit toutefois avoir le rôle serveur de transport Edge ou serveur de transport Hub. Cela s'applique également à une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend le rôle de serveur de transport Edge ou Hub).

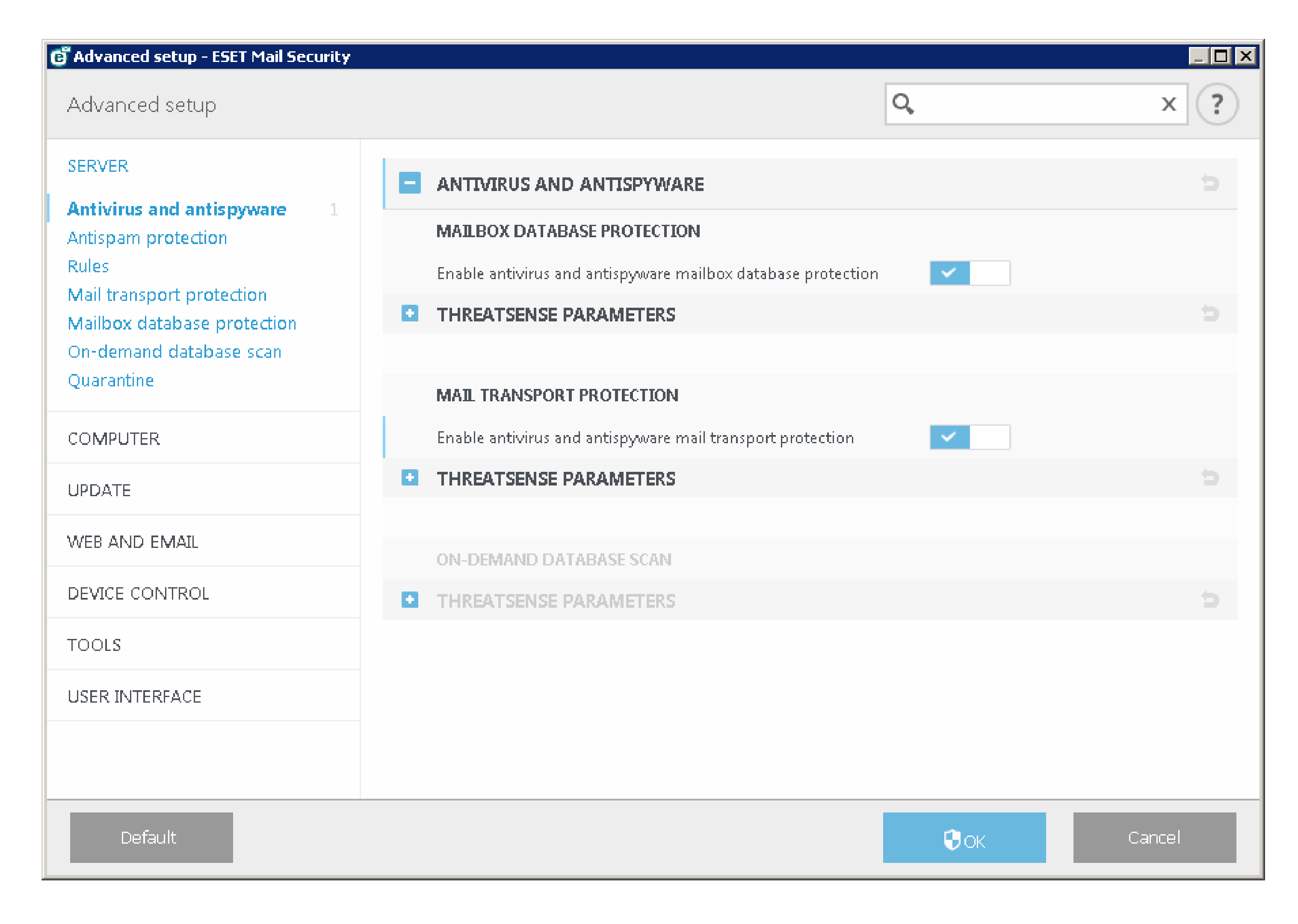
Protection du transport des messages :

Si vous désactivez l'option **Activer la protection antivirus et antispyware du transport des messages**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus sur la couche de transport. Les messages font toujours l'objet d'une recherche de virus et de courrier indésirable sur la couche de base de données et les règles existantes sont appliquées.



Protection de la base de données de boîtes aux lettres :

Si vous désactivez l'option **Activer la protection antivirus et antispyware de la base de données de boîtes aux lettres**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus sur la couche de base de données. Les messages font toujours l'objet d'une recherche de virus et de courrier indésirable sur la couche de base de données et les règles existantes sont appliquées.



5.1.4 Protection antispam

La protection antispam de votre serveur de messagerie est activée par défaut. Pour la désactiver, cliquez sur le commutateur en regard de l'option **Activer la protection antispam**.

Grâce à la fonction **Utiliser les listes blanches Exchange Server pour ignorer automatiquement la protection antispam**, ESET Mail Security peut utiliser les listes blanches spécifiques d'Exchange. Lorsqu'elle est activée, les éléments suivants sont à prendre en compte :

- L'adresse IP du serveur figure dans la liste des adresses IP autorisées du serveur Exchange Server.
- La boîte aux lettres du destinataire du message comporte un indicateur de non-prise en charge de la protection antispam.
- Le destinataire du message dispose de l'adresse de l'expéditeur dans la liste des expéditeurs approuvés (vérifiez que vous avez configuré la synchronisation de la liste des expéditeurs approuvés dans l'environnement de serveur Exchange Server, y compris Agrégation de listes fiables).

Si l'un des cas ci-dessus s'applique à un message entrant, la vérification antispam est ignorée pour ce message. Par conséquent, l'éventuelle nature INDÉSIRABLE de ce message n'est pas évaluée et il est remis à la boîte aux lettres du destinataire.

L'option **Accepter l'indicateur de non-prise en charge de la protection antispam défini sur la session SMTP** est utile si vous avez authentifié les sessions SMTP entre les serveurs Exchange Server avec le paramètre de contournement antispam. Par exemple, si vous avez un serveur Edge et un serveur Hub, il n'est pas nécessaire d'exécuter l'analyse sur le trafic entre ces deux serveurs. L'option **Accepter l'indicateur de non-prise en charge de la protection antispam défini sur la session SMTP** est activée par défaut. Elle n'est toutefois appliquée que si un indicateur de contournement antispam est configuré pour la session SMTP sur le serveur Exchange Server. Si vous désactivez l'option **Accepter l'indicateur de non-prise en charge de la protection antispam défini sur la session SMTP**, ESET Mail Security analyse la session SMTP pour rechercher du courrier indésirable indépendamment du paramètre de contournement antispam sur le serveur Exchange Server.

ℹ **REMARQUE** : la base de données antispam doit être mise à jour régulièrement pour que le module de blocage de courrier indésirable offre la meilleure protection. Pour mettre à jour régulièrement la base de données antispam, vérifiez que ESET Mail Security a accès aux adresses IP correctes sur les ports nécessaires. Pour plus d'informations sur les adresses IP et les ports à activer sur le pare-feu tiers, reportez-vous à cet article de base de connaissances.

5.1.4.1 Filtrage et vérification

Vous pouvez configurer des listes d'éléments **autorisés**, **bloqués** et **ignorés** en spécifiant des critères tels que l'adresse IP ou la plage, le nom de domaine, etc. Pour ajouter, modifier ou supprimer un critère, cliquez sur **Modifier** pour la liste à gérer.

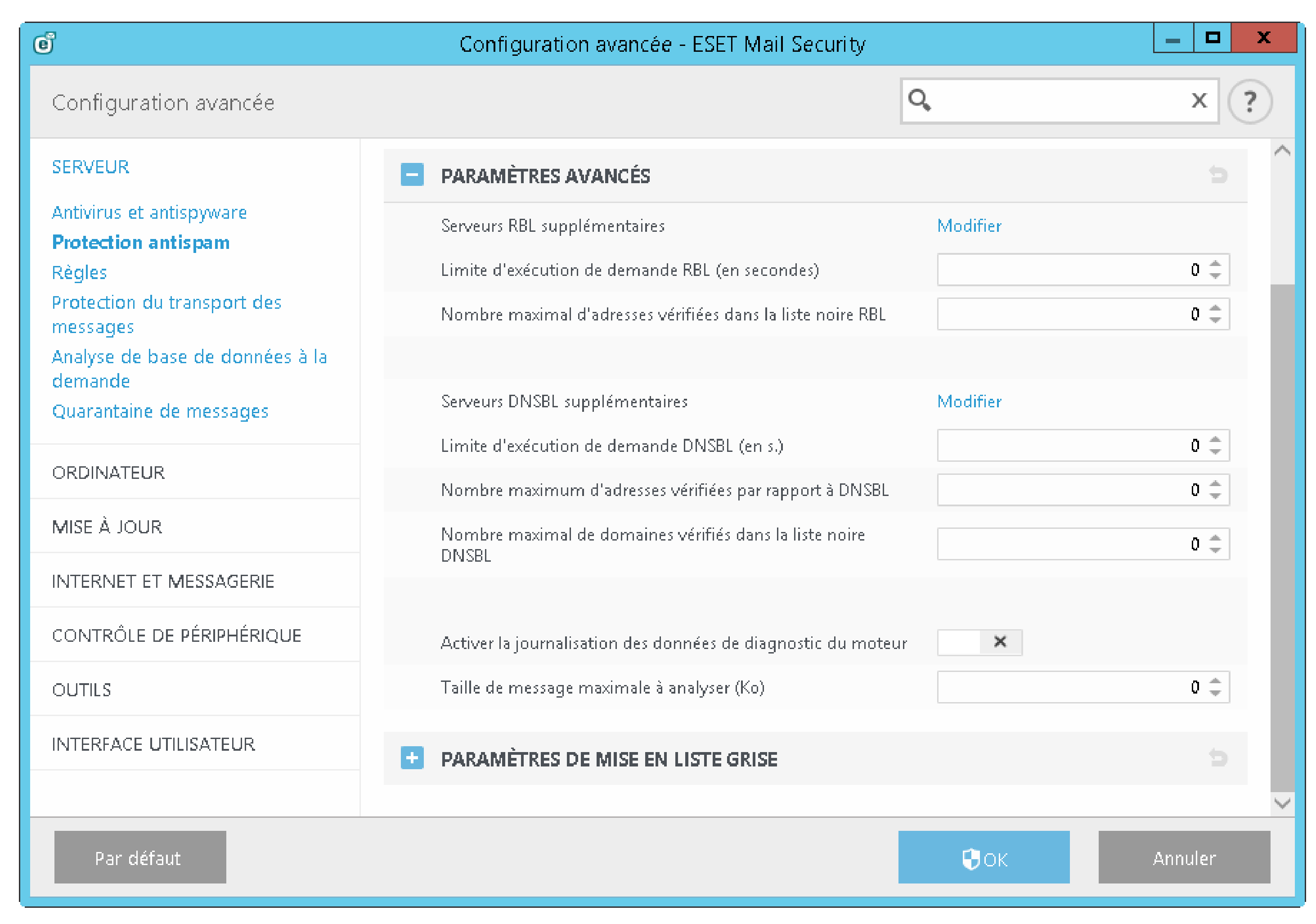
- **Liste des adresses IP approuvées**
- **Liste des adresses IP bloquées**
- **Liste des adresses IP ignorées**
- **Liste des domaines de corps bloqués**
- **Liste des domaines de corps ignorés**
- **Liste des adresses IP de corps bloquées**
- **Liste des adresses IP de corps ignorées**
- **Liste d'expéditeurs approuvés**
- **Liste des expéditeurs bloqués**
- **Domaine approuvé dans la liste des adresses IP**
- **Domaine bloqué dans la liste des adresses IP**
- **Domaine ignoré dans la liste des adresses IP**
- **Liste des jeux de caractères bloqués**
- **Liste des pays bloqués**

5.1.4.2 Paramètres avancés

Ces paramètres permettent la vérification des messages par des serveurs externes (**RBL** - Realtime Blackhole List, **DNSBL** - DNS Blocklist) selon des critères définis.

Limite d'exécution de requête RBL (en secondes) : : cette option vous permet de définir une durée maximale pour les requêtes RBL. Les réponses RBL utilisées sont celles qui proviennent exclusivement des serveurs RBL qui ont répondu dans les temps. Si la valeur est définie sur 0, aucun délai n'est appliqué.

Nombre maximum de domaines vérifiés par rapport à RBL : : cette option vous permet de limiter le nombre d'adresses IP qui sont interrogées sur le serveur RBL. Notez que le nombre total d'interrogations RBL correspond au nombre d'adresses IP figurant dans les en-têtes Reçu (jusqu'à un maximum d'adresses IP maxcheck RBL) multiplié par le nombre de serveurs RBL indiqués dans la liste RBL. Si la valeur est définie sur 0, un nombre illimité d'en-têtes reçus est vérifié. Notez que les adresses IP figurant dans la liste des adresses IP ignorées ne sont pas prises en compte dans la limite des adresses IP RBL.



Limite d'exécution de requête DNSBL (en secondes) : : vous permet de définir un délai maximal pour l'exécution de toutes les requêtes DNSBL.

Nombre maximum d'adresses vérifiées par rapport à DNSBL : : vous permet de limiter le nombre d'adresses IP qui sont interrogées sur le serveur DNS Blocklist.

Nombre maximum de domaines vérifiés par rapport à DNSBL : : vous permet de limiter le nombre de domaines qui sont interrogés sur le serveur DNS Blocklist.

Service RBL : : indique la liste des serveurs RBL (Realtime Blackhole List) à interroger lors de l'analyse des messages. Reportez-vous à la section RBL de ce document pour plus d'informations.

Service DNSBL : : indique la liste des serveurs DNSBL (DNS Blocklist) à interroger, avec les domaines et les adresses IP extraits du corps du message.

Activer la journalisation des données de diagnostic du moteur : écrit des informations détaillées sur le moteur antispam dans les fichiers journaux à des fins de diagnostic.

Taille de message maximale à analyser (Ko) : limite l'analyse antispam des messages plus volumineux que la valeur spécifiée. Ces messages ne sont pas analysés par le moteur antispam.

5.1.4.3 Paramètres de mise en liste grise

La fonction **Activer la mise en liste grise** active une fonctionnalité qui protège les utilisateurs du courrier indésirable à l'aide de la technique suivante : L'agent de transport envoie une valeur de retour SMTP indiquant un rejet temporaire (temporarily reject) (la valeur par défaut est 451/4.7.1) pour tout message qui ne provient pas d'un expéditeur reconnu. Un serveur légitime essaie de renvoyer le message après un délai. Les serveurs de courrier indésirable n'essaient généralement pas de renvoyer le message, car ils envoient des messages à des milliers d'adresses électroniques et ne perdent pas de temps à relancer des expéditions. La mise en liste grise est une couche supplémentaire de protection antispam et n'a aucun effet sur les fonctionnalités d'évaluation du module de blocage de courrier indésirable.

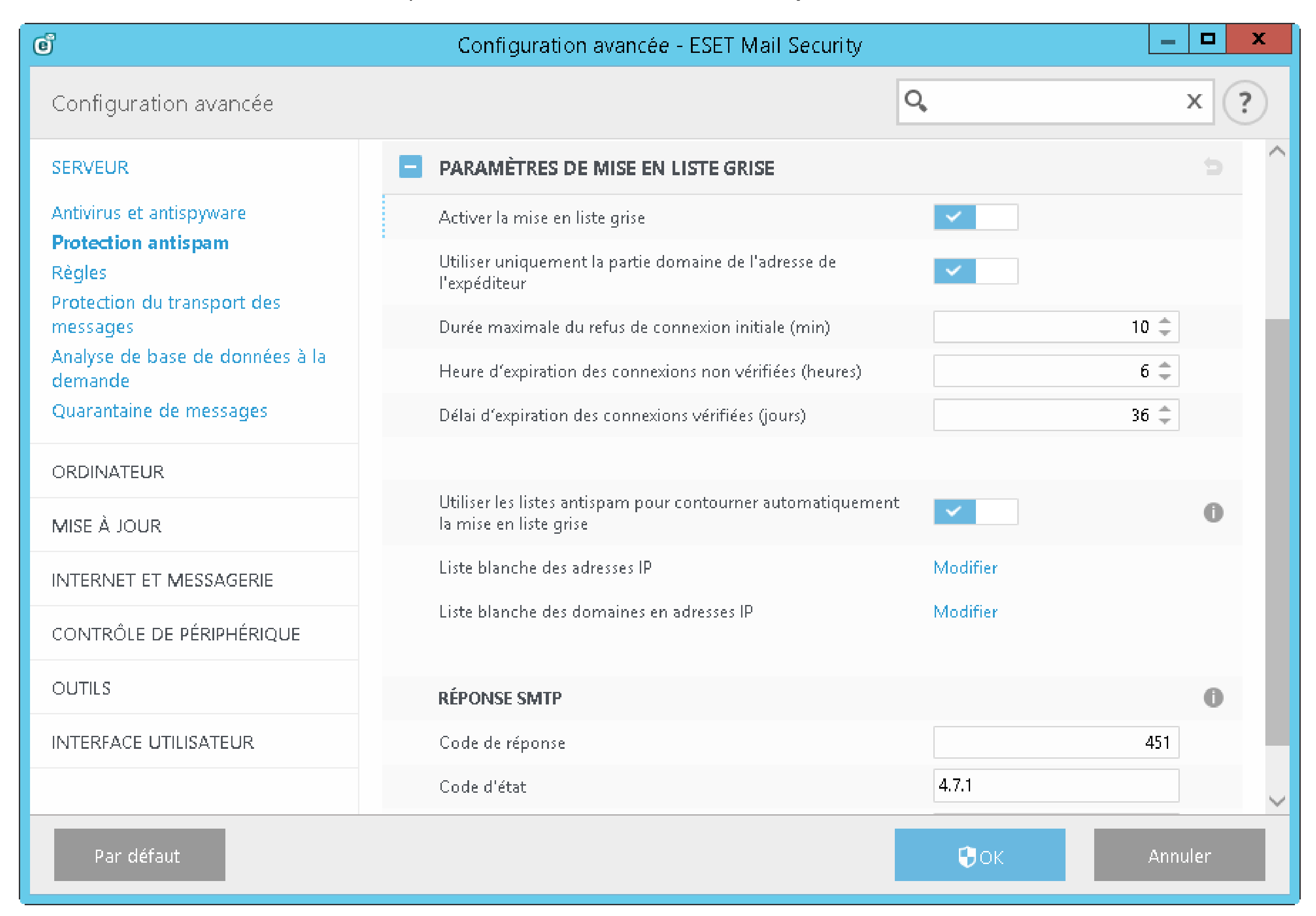
Lors de l'évaluation de la source du message, la méthode de mise en liste grise prend en compte les listes d'**adresses IP approuvées**, **ignorées**, **autorisées** et d'**expéditeurs sûrs** sur le serveur Exchange et les paramètres AntispamBypass de la boîte aux lettres du destinataire. Les messages de ces listes d'adresses IP/d'expéditeurs ou ceux remis à une boîte aux lettres dont l'option AntispamBypass est activée sont ignorés par la méthode de détection de mise en liste grise.

Utiliser uniquement la partie domaine de l'adresse de l'expéditeur : ignore le nom du destinataire dans l'adresse électronique ; seul le domaine est pris en compte.

Durée limite du refus de connexion initial (min) : lorsqu'un message est remis pour la première fois et qu'il est refusé temporairement, ce paramètre définit la période pendant laquelle le message est toujours refusé (mesuré depuis le premier refus). Une fois la période écoulée, le message est reçu correctement. La valeur minimum que vous entrez est de 1 minute.

Durée avant expiration des connexions non vérifiées (heures) : ce paramètre définit l'intervalle minimum pendant lequel les données de triplet sont stockées. Un serveur valide doit renvoyer un message souhaité avant l'expiration de cette période. Cette valeur doit être supérieure à la valeur **Durée limite du refus de connexion initial**.

Durée avant expiration des connexions vérifiées (jours) : nombre minimum de jours pendant lesquels les informations de triplet doivent être stockées et pendant lesquels les messages d'un expéditeur défini sont reçus sans délai. Cette valeur doit être supérieure à la valeur **Durée avant expiration des connexions non vérifiées**.



Réponse SMTP (pour les connexions refusées temporairement) : vous pouvez spécifier un **code de réponse**, un **code d'état** et un **message de réponse**, qui définissent la réponse de refus temporaire SMTP envoyée au serveur SMTP si un message est refusé.

Exemple de message de réponse de rejet SMTP :

Code de réponse	Code d'état	Message de réponse
451	4.7.1	Requested action aborted: local error in processing (Action demandée interrompue : erreur locale en cours de traitement)

AVERTISSEMENT : une syntaxe incorrecte des codes de réponses SMTP peut provoquer un dysfonctionnement de la protection par mise en liste grise. En conséquence, les messages de courrier indésirable peuvent être remis à des clients ou des messages ne peuvent pas être délivrés du tout.

REMARQUE : vous pouvez également utiliser des variables système lors de la définition de la réponse SMTP de rejet.

5.1.5 Règles

Les **règles** permettent aux administrateurs de définir manuellement les conditions de filtrage des messages électroniques et les actions à exécuter sur les messages électroniques filtrés.

Il existe trois ensembles de règles distincts. Les règles disponibles dans votre système dépendent de la version de Microsoft Exchange Server installée avec ESET Mail Security sur le serveur.:

- Protection de la base de données des boîtes aux lettres - Ce type de protection est uniquement disponible pour Microsoft Exchange Server 2010, 2007 et 2003 avec le rôle serveur de boîte aux lettres (Microsoft Exchange 2010 et 2007) ou serveur principal (Microsoft Exchange 2003). Ce type d'analyse peut être effectué sur une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend le rôle de serveur de boîte aux lettres ou de serveur principal).
- Protection du transport des messages - Cette protection est assurée par l'agent de transport et est uniquement disponible pour Microsoft Exchange Server 2007 ou version ultérieure avec le rôle serveur de transport Edge ou serveur de transport Hub. Ce type d'analyse peut être effectué sur une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend un des rôles de serveur indiqués).
- Analyse de base de données à la demande - Permet d'exécuter ou de planifier une analyse de la base de données de boîtes aux lettres Exchange. Cette fonctionnalité est uniquement disponible pour Microsoft Exchange Server 2007 ou version ultérieure avec le rôle serveur de boîte aux lettres ou serveur de transport Hub. Ce type d'analyse s'applique également à une seule installation de serveur avec plusieurs rôles Exchange Server sur un ordinateur (s'il comprend un des rôles de serveur indiqués). Pour plus d'informations sur les rôles d'Exchange 2013, consultez Rôles Exchange Server 2013.

5.1.5.1 Liste des règles

Une règle est composée de **conditions** et d'**actions**. Une fois que toutes les conditions d'un message électronique sont remplies, les actions sont exécutées sur celui-ci. En d'autres termes, les règles sont appliquées en fonction d'un ensemble de conditions combinées. Si plusieurs conditions sont associées à une règle, elles sont combinées à l'aide de l'opérateur logique ET et la règle n'est appliquée que lorsque les conditions sont réunies.

La fenêtre Liste **des règles** affiche les règles existantes. Les règles sont classées dans trois niveaux et évaluées dans cet ordre :

- **Règles de filtrage (1)**
- **Règles de traitement des pièces jointes (2)**
- **Règles de traitement des résultats (3)**

Les règles d'un même niveau sont évaluées dans le même ordre que celui de leur affichage dans la fenêtre Règles. Vous pouvez uniquement modifier l'ordre des règles d'un même niveau. Par exemple, si vous disposez de plusieurs règles de filtrage, vous pouvez modifier l'ordre de leur application. Vous ne pouvez pas modifier leur ordre en plaçant les règles de traitement des pièces jointes avant les règles de filtrage (les boutons Monter/Descendre ne sont pas disponibles). En d'autres termes, vous ne pouvez pas mélanger des règles de niveaux différents.

La colonne Correspondances affiche le nombre de fois que la règle a été appliquée. Si vous décochez une case (à gauche du nom de chaque règle), la règle correspondante est désactivée jusqu'à ce que vous recochiez la case.

- **Ajouter...** : ajoute une nouvelle règle.
- **Modifier...** : modifie une règle existante.
- **Supprimer** : supprime une règle sélectionnée.
- **Monter** : déplace la règle sélectionnée vers le haut de la liste.
- **Descendre** : déplace la règle sélectionnée vers le bas de la liste.
- **Réinitialiser** : réinitialise le compteur de règles (colonne Correspondances).

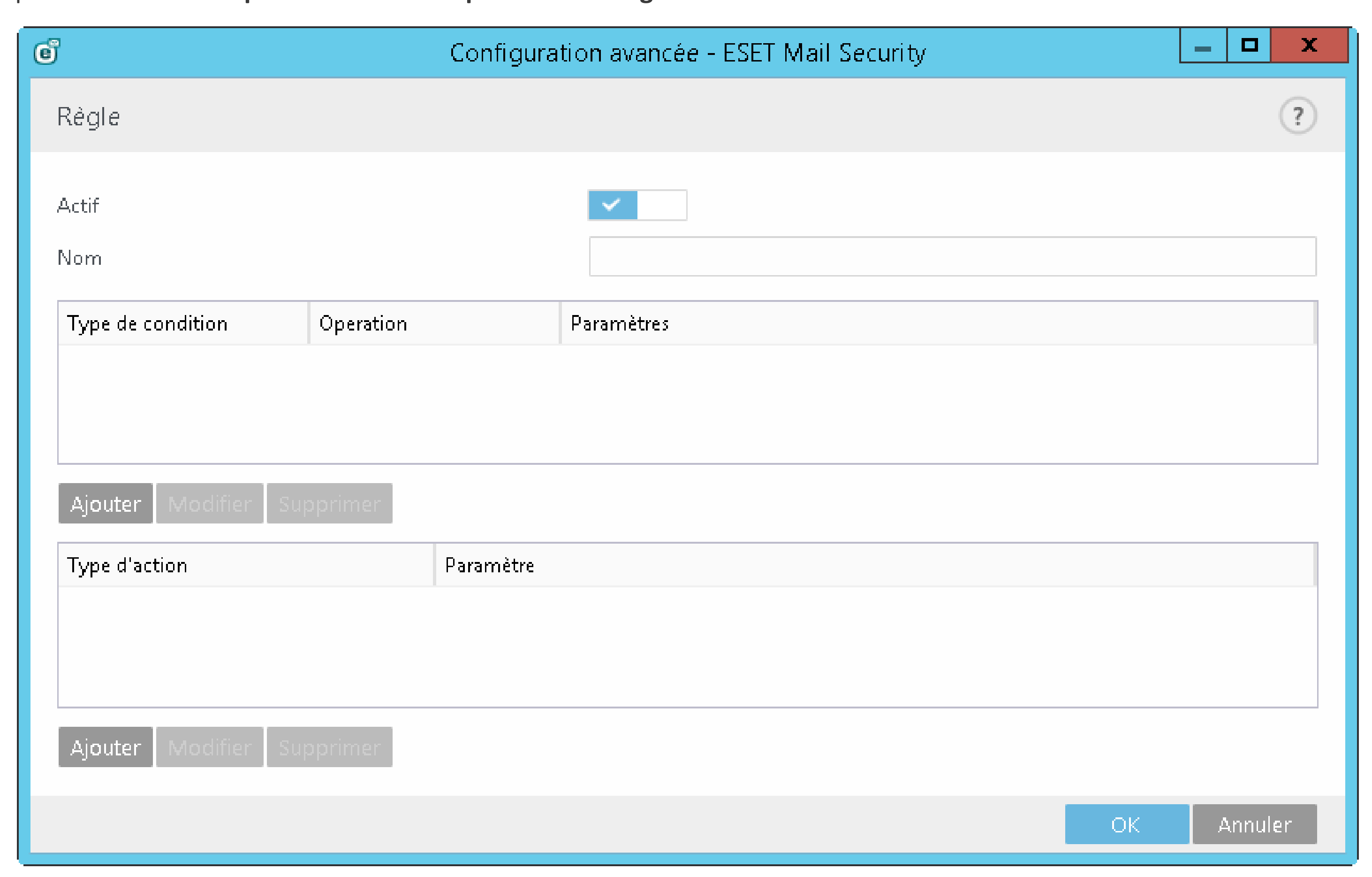
i **REMARQUE** : si une nouvelle règle est ajoutée ou une règle existante est modifiée, une nouvelle analyse des messages démarre automatiquement à l'aide des règles créées/modifiées.

Les règles permettent de vérifier un message lorsque celui est traité par l'agent de transport ou VSAPI. Si les deux méthodes, agent de transport et VSAPI, sont activées et que le message correspond aux conditions de la règle, le nombre de règles peut augmenter de 2 ou plus. Le système VSAPI accède en effet séparément au corps et à la pièce jointe d'un message, ce qui signifie que les règles sont appliquées à chacune de ces parties. Les règles sont également appliquées lors de l'analyse en arrière-plan (lorsque ESET Mail Security effectue par exemple une analyse des boîtes aux lettres suite au téléchargement d'une nouvelle base des signatures de virus), ce qui peut augmenter le compteur de règles.

5.1.5.1.1 Assistant Règle

Vous pouvez définir des **conditions** et des **actions** à l'aide de l'assistant **Règle**. Définissez d'abord les conditions, puis les actions. Cliquez sur **Ajouter** pour afficher la fenêtre Condition de règle dans laquelle vous pouvez sélectionner un type de condition, une opération et une valeur. À ce stade, vous pouvez ajouter une action de règle. Une fois les conditions et les actions définies, saisissez un **nom** pour la règle (un nom significatif vous permettant de reconnaître la règle). Ce nom sera affiché dans la liste des règles. Si vous souhaitez préparer des règles en vue d'une utilisation ultérieure, vous pouvez cliquer sur le commutateur en regard de l'option **Active** pour désactiver la règle. Pour activer une règle, cochez la case en regard de celle-ci dans la liste des règles.

Certaines **conditions** et **actions** sont différentes pour les règles propres à la **protection du transport des messages**, à la **protection de la base de données de boîtes aux lettres** et à l'**analyse de base de données à la demande**. Chaque type de protection utilise en effet une approche un peu différente lors du traitement des messages, tout particulièrement la **protection du transport des messages**.



5.1.5.1.1.1 Condition de règle

Cet assistant permet d'ajouter des conditions pour une règle. Sélectionnez **Type** > **Opération** dans la liste déroulante (la liste des opérations change en fonction du type de règle sélectionné), puis **Paramètre**. Les champs de paramètre changent en fonction du type de règle et de l'opération.

Choisissez par exemple **Taille de la pièce jointe** > **est supérieur à** , puis, sous **Paramètre**, spécifiez 10 Mo. Avec ces paramètres, un message qui contient une pièce jointe dont la taille est supérieure à 10 Mo est traité à l'aide de l'action de règle que vous avez spécifiée. Pour cette raison, vous devez spécifier une action à entreprendre lorsqu'une règle donnée est déclenchée si vous ne l'avez pas fait lors de la définition des paramètres de cette règle.

i **REMARQUE :** il est possible d'ajouter plusieurs conditions pour une règle. Lors de l'ajout de plusieurs conditions, les conditions qui s'annulent mutuellement ne sont pas affichées.

Les **conditions** suivantes sont disponibles pour la **protection du transport des messages** (certaines options peuvent ne pas s'afficher selon les conditions précédemment sélectionnées) :

- **Objet** : s'applique aux messages qui contiennent ou non une chaîne spécifique (ou une expression régulière) dans l'objet.
- **Expéditeur** : s'applique aux messages envoyés par un expéditeur spécifique.
- **Destinataire** : s'applique aux messages envoyés à un destinataire spécifique.
- **Nom de la pièce jointe** : s'applique aux messages qui contiennent des pièces jointes avec un nom spécifique.
- **Taille de la pièce jointe** : s'applique aux messages dont la pièce jointe ne correspond pas à la taille spécifiée, se trouve dans la plage de tailles spécifiée ou dépasse la taille spécifiée.
- **Type de la pièce jointe** : s'applique aux messages avec un type de fichier joint spécifique. Les types de fichier sont classés dans des groupes pour une sélection aisée. Vous pouvez sélectionner plusieurs types de fichier ou des catégories entières.
- **Taille du message** : s'applique aux messages dont les pièces jointes ne correspondent pas à la taille spécifiée, se trouvent dans la plage de tailles spécifiée ou dépassent la taille spécifiée.
- **Résultat de l'analyse antispam** : s'applique aux messages marqués ou non comme étant indésirables ou légitimes.
- **Résultat de l'analyse antivirus** : s'applique aux messages marqués comme étant malveillants ou non.
- **Message interne** : s'applique selon qu'un message est interne ou non.
- **Heure de réception** : s'applique aux messages reçus avant ou après une date spécifique ou dans une plage de dates spécifique.
- **En-têtes de message** : s'applique aux messages contenant des données spécifiques dans l'en-tête.
- **Contient une archive protégée par mot de passe** : s'applique aux messages dont les pièces jointes d'archive sont protégées par mot de passe.
- **Contient une archive endommagée** : s'applique aux messages dont les pièces jointes d'archive sont endommagées (qui ne peuvent généralement pas être ouvertes).
- **Adresse IP de l'expéditeur** : s'applique aux messages envoyés à partir d'une adresse IP spécifique.
- **Domaine de l'expéditeur** : s'applique aux messages provenant d'un expéditeur avec un domaine spécifique dans son adresse électronique.

- **Unités d'organisation du destinataire** : s'applique aux messages envoyés à un destinataire d'une unité d'organisation spécifique.

Les conditions suivantes sont disponibles pour la protection de la base de données de boîtes aux lettres et l'analyse de base de données à la demande (certaines options peuvent ne pas s'afficher selon les conditions précédemment sélectionnées) :

- **Objet** : s'applique aux messages qui contiennent ou non une chaîne spécifique (ou une expression régulière) dans l'objet.
- **Expéditeur** : s'applique aux messages envoyés par un expéditeur spécifique.
- **Destinataire** : s'applique aux messages envoyés à un destinataire spécifique.
- **Boîte aux lettres** : s'applique aux messages situés dans une boîte aux lettres spécifique.
- **Nom de la pièce jointe** : s'applique aux messages qui contiennent des pièces jointes avec un nom spécifique.
- **Taille de la pièce jointe** : s'applique aux messages dont la pièce jointe ne correspond pas à la taille spécifiée, se trouve dans la plage de tailles spécifiée ou dépasse la taille spécifiée.
- **Type de la pièce jointe** : s'applique aux messages avec un type de fichier joint spécifique. Les types de fichier sont classés dans des groupes pour une sélection aisée. Vous pouvez sélectionner plusieurs types de fichier ou des catégories entières.
- **Résultat de l'analyse antivirus** : s'applique aux messages marqués comme étant malveillants ou non.
- **Heure de réception** : s'applique aux messages reçus avant ou après une date spécifique ou dans une plage de dates spécifique.
- **En-têtes de message** : s'applique aux messages contenant des données spécifiques dans l'en-tête.
- **Contient une archive protégée par mot de passe** : s'applique aux messages dont les pièces jointes d'archive sont protégées par mot de passe.
- **Contient une archive endommagée** : s'applique aux messages dont les pièces jointes d'archive sont endommagées (qui ne peuvent généralement pas être ouvertes).
- **Adresse IP de l'expéditeur** : s'applique aux messages envoyés à partir d'une adresse IP spécifique.
- **Domaine de l'expéditeur** : s'applique aux messages provenant d'un expéditeur avec un domaine spécifique dans son adresse électronique.

5.1.5.1.1.2 Action de règle

Vous pouvez ajouter des actions qui seront entreprises sur des messages et/ou des pièces jointes et qui correspondent aux conditions de règle.

i **REMARQUE :** il est possible d'ajouter plusieurs conditions pour une règle. Lors de l'ajout de plusieurs conditions, les conditions qui s'annulent mutuellement ne sont pas affichées.

Les **actions** suivantes sont disponibles pour la **protection du transport des messages** (certaines options peuvent ne pas s'afficher selon les conditions précédemment sélectionnées) :

- **Mettre le message en quarantaine** : le message ne sera pas remis au destinataire et sera déplacé vers la quarantaine des messages.
- **Supprimer la pièce jointe** : supprime la pièce jointe d'un message. Le message sera remis au destinataire sans la pièce jointe.
- **Refuser le message** : le message ne sera pas remis et un rapport de non-remise sera envoyé à l'expéditeur.
- **Supprimer le message en silence** : supprime un message sans envoyer de rapport de non-remise.

- **Définir la valeur SCL** : modifie ou définie une valeur SCL spécifique.
- **Envoyer le rapport** : envoie un rapport.
- **Ignorer l'analyse antispam** : le message sera analysé par le moteur antispam.
- **Ignorer l'analyse antivirus** : le message sera analysé par le moteur antivirus.
- **Évaluer d'autres règles** : permet l'évaluation d'autres règles afin que l'utilisateur puisse définir plusieurs ensembles de conditions et d'actions à entreprendre en fonction de ces conditions.
- **Consigner** : écrit des informations sur la règle appliquée dans le journal de l'application.
- **Ajouter un champ d'en-tête** : ajoute une chaîne personnalisée à un en-tête de message.

Les **actions** suivantes sont disponibles pour la **protection de la base de données de boîtes aux lettres** et l'**analyse de base de données à la demande** (certaines options peuvent ne pas s'afficher selon les conditions précédemment sélectionnées) :

- **Supprimer la pièce jointe** : supprime la pièce jointe d'un message. Le message sera remis au destinataire sans la pièce jointe.
- **Mettre en quarantaine la pièce jointe** : place la pièce jointe au message dans la quarantaine des messages. Le message électronique sera remis au destinataire sans la pièce jointe.
- **Remplacer la pièce jointe par des informations sur l'action** : supprime une pièce jointe et ajoute des informations sur l'action entreprise sur la pièce jointe au corps du message.
- **Supprimer le message** : supprime le message.
- **Envoyer le rapport** : envoie un rapport.
- **Ignorer l'analyse antivirus** : le message sera analysé par le moteur antivirus.
- **Évaluer d'autres règles** : permet l'évaluation d'autres règles afin que l'utilisateur puisse définir plusieurs ensembles de conditions et d'actions à entreprendre en fonction de ces conditions.
- **Consigner** : écrit des informations sur la règle appliquée dans le journal de l'application.
- **Déplacer le message vers la corbeille** (uniquement disponible pour l'**analyse de base de données à la demande**) : place un message électronique dans la corbeille du côté du client de messagerie.

5.1.6 Protection de la base de données de boîtes aux lettres

La fonctionnalité **Protection de la base de données de boîtes aux lettres**, accessible dans **Paramètres avancés** > **Serveur**, est disponible pour les systèmes suivants :

- Microsoft Exchange Server 2003 (rôle de serveur principal)
- Microsoft Exchange Server 2003 (installation de serveur unique avec plusieurs rôles)
- Microsoft Exchange Server 2007 (rôle de serveur de boîtes aux lettres)
- Microsoft Exchange Server 2007 (installation de serveur unique avec plusieurs rôles)
- Microsoft Exchange Server 2010 (rôle de serveur de boîtes aux lettres)
- Microsoft Exchange Server 2010 (installation de serveur unique avec plusieurs rôles)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

REMARQUE : la protection de la base de données de boîtes aux lettres n'est pas disponible pour Microsoft Exchange Server 2013.

Si vous désélectionnez l'option **Activer la protection antivirus et antispyware VSAPI 2.6**, le plugin ESET Mail Security du serveur Exchange n'est pas déchargé depuis le processus du serveur Microsoft Exchange. Il passe uniquement en revue les messages sans rechercher les virus. En revanche, les messages font l'objet d'une recherche de courrier

indésirable et les règles sont appliquées.

Si l'option **Analyse proactive** est activée, les nouveaux messages entrants sont analysés dans l'ordre dans lequel ils ont été reçus. Si cette option est activée et qu'un utilisateur ouvre un message qui n'a pas encore été analysé, ce message est analysé avant les autres messages dans la file d'attente.

L'option **Analyse en arrière-plan** permet l'exécution de l'analyse de tous les messages en arrière-plan (l'analyse s'exécute dans le magasin des boîtes aux lettres et des dossiers publics, comme la base de données Exchange). En fonction de différents facteurs tels que la charge actuelle du système, le nombre d'utilisateurs actifs, etc., Microsoft Exchange Server décide si une analyse en arrière-plan doit s'exécuter, et conserve la liste des messages analysés et de la version de la base des signatures de virus utilisée. Si vous ouvrez un message qui n'a pas été analysé par la base des signatures de virus la plus à jour, Microsoft Exchange Server envoie le message à ESET Mail Security pour qu'il soit analysé avant d'être ouvert dans le client de messagerie. Vous pouvez choisir d'**analyser uniquement les messages avec pièce jointe** et de les filtrer en fonction de leur heure de réception à l'aide des options **Niveau d'analyse** suivantes :

- **Tous les messages**
- **Messages reçus au cours de l'année dernière**
- **Messages reçus au cours des 6 derniers mois**
- **Messages reçus au cours des 3 derniers mois**
- **Messages reçus au cours du dernier mois**
- **Messages reçus au cours de la semaine dernière**

L'analyse en arrière-plan pouvant avoir un impact sur la charge du système (elle est effectuée après chaque mise à jour de la base des signatures des virus), il est recommandé de planifier cette analyse en dehors des heures de travail. L'analyse en arrière-plan planifiée peut être configurée par l'intermédiaire d'une tâche spécifique dans le Planificateur. Lorsque vous planifiez une analyse en arrière-plan, vous pouvez définir l'heure de son lancement, le nombre de répétitions et d'autres paramètres disponibles dans le Planificateur. Une fois planifiée, la tâche apparaît dans la liste des tâches planifiées ; vous pouvez modifier ses paramètres, la supprimer ou la désactiver temporairement.

L'activation de l'option **Analyser le corps des messages RTF** active l'analyse des corps de messages RTF. Les corps de ces messages RTF peuvent contenir des macrovirus.

REMARQUE : les corps des messages en texte brut ne sont pas analysés par VSAPI.

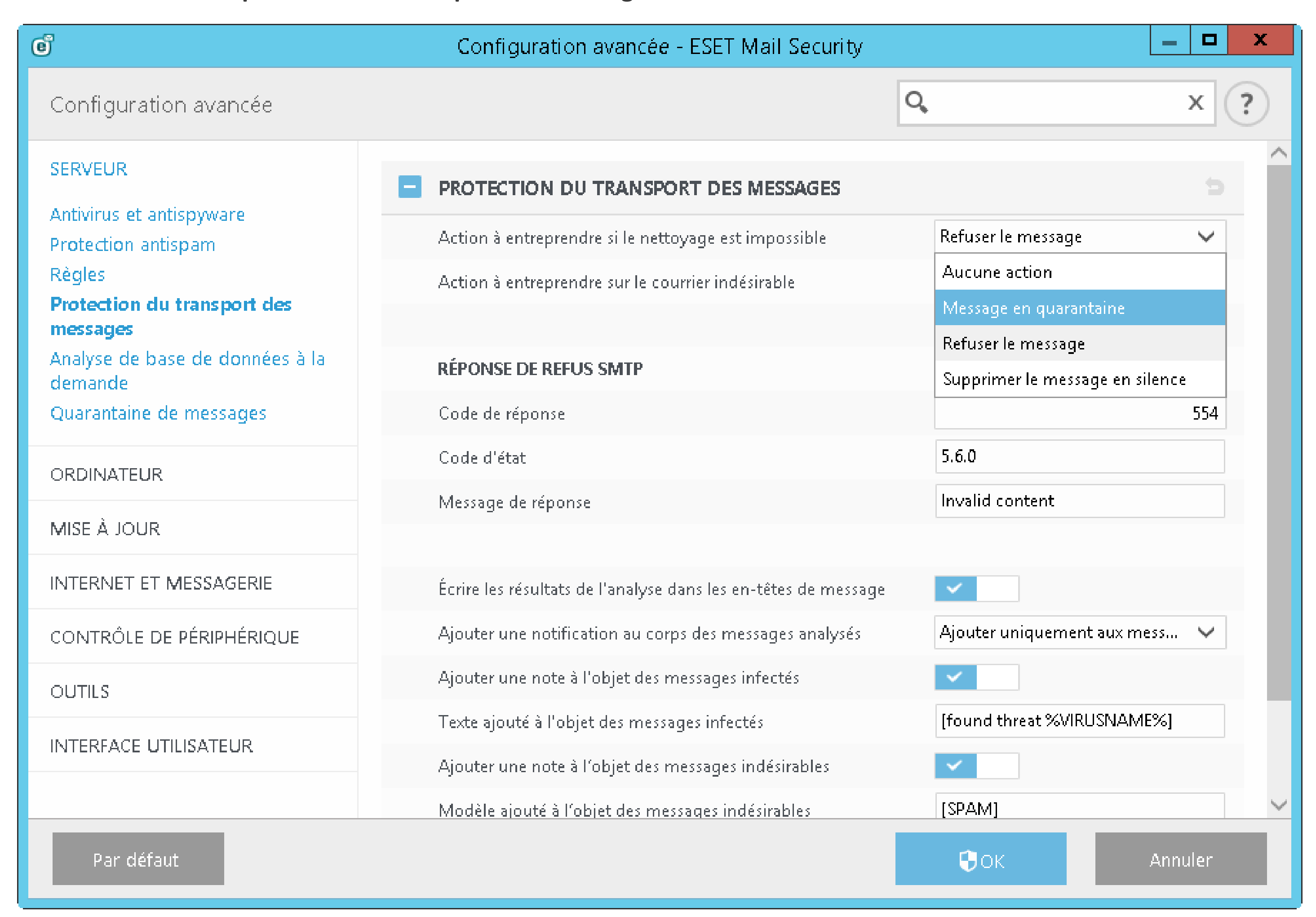
REMARQUE : les dossiers publics sont traités comme les boîtes aux lettres. Cela signifie qu'ils sont également analysés.

5.1.7 Protection du transport des messages

La fonctionnalité **Protection du transport des messages**, accessible dans **Paramètres avancés** > **Serveur**, est disponible pour les systèmes d'exploitation suivants :

- Microsoft Exchange Server 2007 (serveur de transport Edge ou serveur de transport Hub)
- Microsoft Exchange Server 2007 (installation de serveur unique avec plusieurs rôles)
- Microsoft Exchange Server 2010 (serveur de transport Edge ou serveur de transport Hub)
- Microsoft Exchange Server 2010 (installation de serveur unique avec plusieurs rôles)
- Microsoft Exchange Server 2013 (rôle de serveur de transport Edge)
- Microsoft Exchange Server 2013 (installation de serveur unique avec plusieurs rôles)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

Paramètres de la protection du transport des messages :



L'action antivirus sur la couche de transport peut être définie dans **Action à entreprendre si le nettoyage n'est pas possible** :

- **Aucune action :** permet de conserver les messages infectés qui ne peuvent pas être nettoyés.
- **Mettre le message en quarantaine :** permet d'envoyer les messages infectés à la boîte aux lettres de quarantaine.
- **Refuser le message :** permet de refuser un message infecté.
- **Supprimer le message en silence** : permet de supprimer les messages sans envoyer de rapport de non-remise.

L'action antispam sur la couche de transport peut être définie dans **Action à entreprendre sur les messages de courrier indésirable** :

- **Aucune action** : permet de conserver le message même s'il est marqué comme étant du courrier indésirable.
- **Mettre le message en quarantaine** : permet d'envoyer les messages marqués comme étant du courrier indésirable à la boîte aux lettres de quarantaine.
- **Refuser le message :** permet de refuser les messages marqués comme étant indésirables.
- **Supprimer le message en silence** : permet de supprimer les messages sans envoyer de rapport de non-remise.

Réponse de refus SMTP : vous pouvez spécifier un **code de réponse**, un **code d'état** et un **message de réponse**, qui définissent la réponse de refus temporaire SMTP envoyée au serveur SMTP si un message est refusé.

Lors de la suppression des messages, envoyer une réponse de refus SMTP :

- Si cette option n'est pas sélectionnée, le serveur envoie une réponse SMTP favorable à l'agent de transfert de message (MTA) de l'expéditeur au format '250 2.5.0 : Requested mail action okay, completed' ('250 2.5.0 : action demandée sur courrier OK, terminée'), puis effectue une suppression automatique.
- Si l'option est sélectionnée, une réponse de refus SMTP est renvoyée à l'agent de transfert de message (MTA) de l'expéditeur. Vous pouvez saisir un message de réponse au format suivant :

Code principal de réponse	Code d'état complémentaire	Description

250	2.5.0	Requested mail action okay, completed (Action demandée sur courrier OK, terminée)
451	4.5.1	Requested action aborted:local error in processing (Action demandée abandonnée : erreur locale dans le traitement)
550	5.5.0	Requested action not taken:mailbox unavailable (Action demandée non entreprise : boîte aux lettres indisponible)
554	5.6.0	Invalid content (Contenu non valide)

i **REMARQUE :** vous pouvez également utiliser des variables système pour configurer des réponses de rejet SMTP.

L'option **Ajouter une notification au corps des messages analysés** propose trois options :
- Ne pas ajouter aux messages
- Ajouter uniquement aux messages infectés
- Ajouter à tous les messages analysés (ne s'applique pas aux messages internes)

Ajouter une note à l'objet des messages infectés : lorsque cette option est activée, ESET Mail Security ajoute une notification à l'objet du message dont la valeur est définie dans le champ de texte **Modèle ajouté à l'objet des messages indésirables** (le texte prédéfini par défaut est [SPAM]). Cette modification peut être utilisée pour automatiser le filtrage du courrier indésirable en filtrant les messages avec un objet spécifique, à l'aide par exemple de règles ou du côté client (si cette option est prise en charge par le client de messagerie) pour placer ces messages dans un dossier distinct.

i **REMARQUE :** lors de la modification de texte, vous pouvez également utiliser des variables système qui seront ajoutées à l'objet.

5.1.7.1 Paramètres avancés

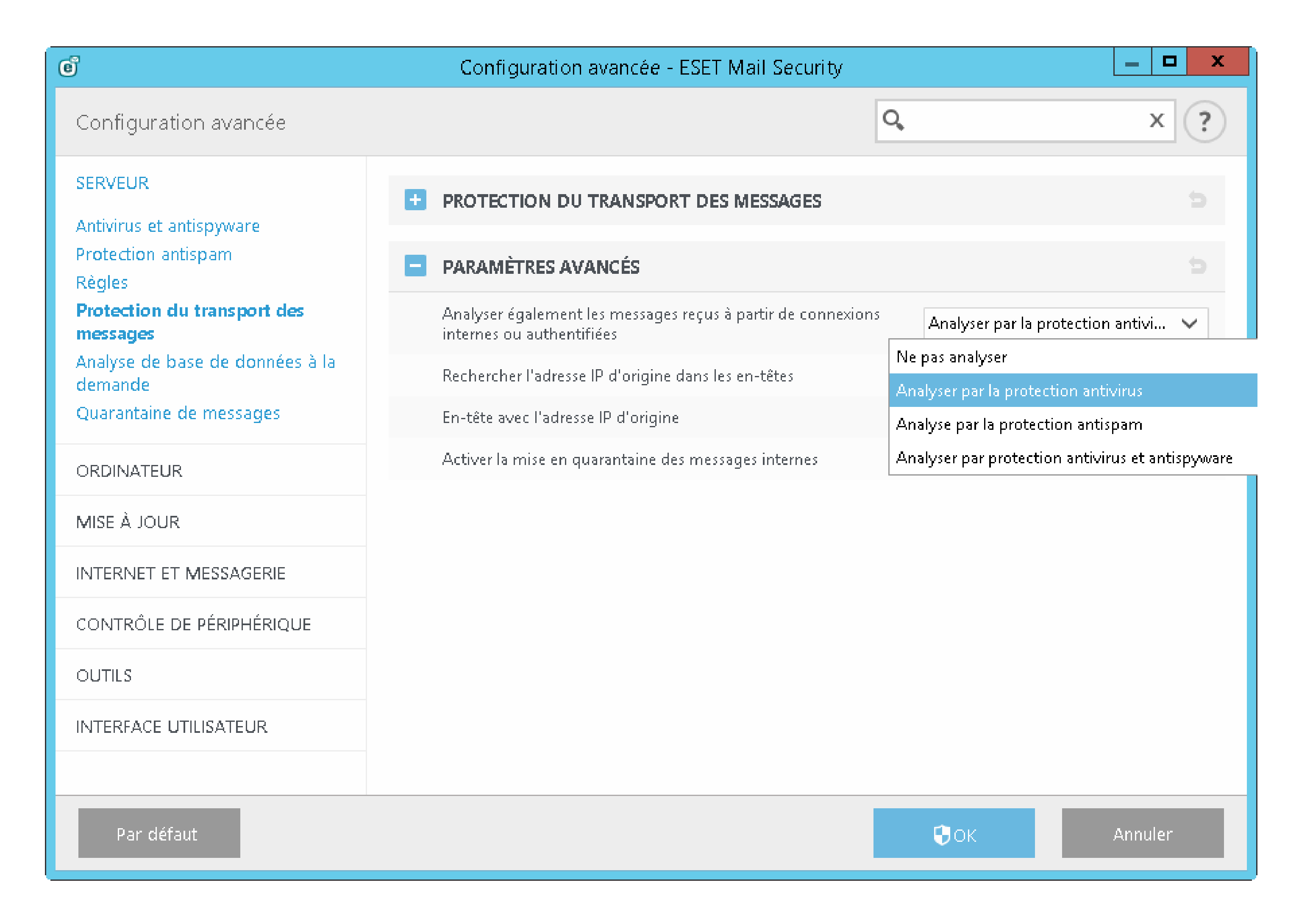
Dans cette section, vous pouvez modifier les paramètres appliqués pour l'agent de transport :

- **Analyser également les messages reçus de connexions authentifiées ou internes** : vous pouvez choisir le type d'analyse à effectuer sur les messages reçus des sources authentifiées ou des serveurs locaux. L'analyse de ces messages est conseillée car elle optimise la protection. Elle est toutefois nécessaire si vous utilisez le connecteur POP3 intégré de Microsoft SBS pour récupérer les messages électroniques des serveurs POP3 externes ou des services de messagerie (**Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem**, par exemple). Pour plus d'informations, reportez-vous à la section Connecteur POP3 et protection antispam.

- **Rechercher l'adresse IP d'origine dans les en-têtes** : lorsque cette option est activée, ESET Mail Security recherche l'adresse IP d'origine dans les en-têtes des messages pour que différents modules de protection (antispam et autres) puissent l'utiliser. Si votre organisation Exchange est séparée d'Internet par un proxy, une passerelle ou un serveur de transport Edge, les messages électroniques semblent provenir d'une seule adresse IP (généralement une adresse interne). Il est courant que sur le serveur extérieur (serveur de transport Edge dans DMZ, par exemple) où l'adresse IP des expéditeurs est connue, cette adresse IP est écrite dans les en-têtes du message reçu. La valeur spécifiée dans le champ **En-tête avec l'adresse IP d'origine** ci-dessous correspond à l'en-tête recherché par ESET Mail Security dans les en-têtes des messages.

- **En-tête avec l'adresse IP d'origine** : correspond à l'en-tête recherché par ESET Mail Security dans les en-têtes des messages. La valeur par défaut est **Adresse IP-origine-X**. Remplacez cette valeur par celle qui convient si vous utilisez des outils tiers ou personnalisés qui utilisent un autre en-tête.

- **Activer la mise en quarantaine des messages internes** : lorsque cette option est activée, les messages internes sont mis en quarantaine.



5.1.8 Analyse de base de données à la demande

L'**analyse de base de données à la demande** est disponible pour les systèmes suivants :

- Microsoft Exchange Server 2007 (serveur de boîtes aux lettres ou serveur de transport Hub)
- Microsoft Exchange Server 2007 (installation de serveur unique avec plusieurs rôles)
- Microsoft Exchange Server 2010 (serveur de boîtes aux lettres ou serveur de transport Hub)
- Microsoft Exchange Server 2010 (installation de serveur unique avec plusieurs rôles)
- Microsoft Exchange Server 2013 (rôle de serveur de boîtes aux lettres)
- Microsoft Exchange Server 2013 (installation de serveur unique avec plusieurs rôles)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

REMARQUE : si vous exécutez Microsoft Exchange Server 2007 ou 2010 vous pouvez choisir entre la protection de la base de données de boîtes aux lettres et une analyse de base de données à la demande. Sachez toutefois qu'une seule de ces deux protections peut être active à la fois. Si vous choisissez d'utiliser l'analyse de base de données à la demande, vous devez désactiver l'intégration de la protection de la base de données de boîtes aux lettres dans Configuration avancée, sous Serveur. Dans le cas contraire, Analyse de base de données à la demande ne sera pas disponible.

Paramètres d'analyse de base de données à la demande :

Adresse de l'hôte : nom ou adresse IP du serveur exécutant les services Web Exchange.

Nom d'utilisateur : indiquez les informations d'identification de l'utilisateur qui dispose d'un accès adéquat aux services Web Exchange.

Mot de passe de l'utilisateur : cliquez sur **Définir** en regard de **Mot de passe de l'utilisateur**, puis saisissez le mot de passe de ce compte d'utilisateur.

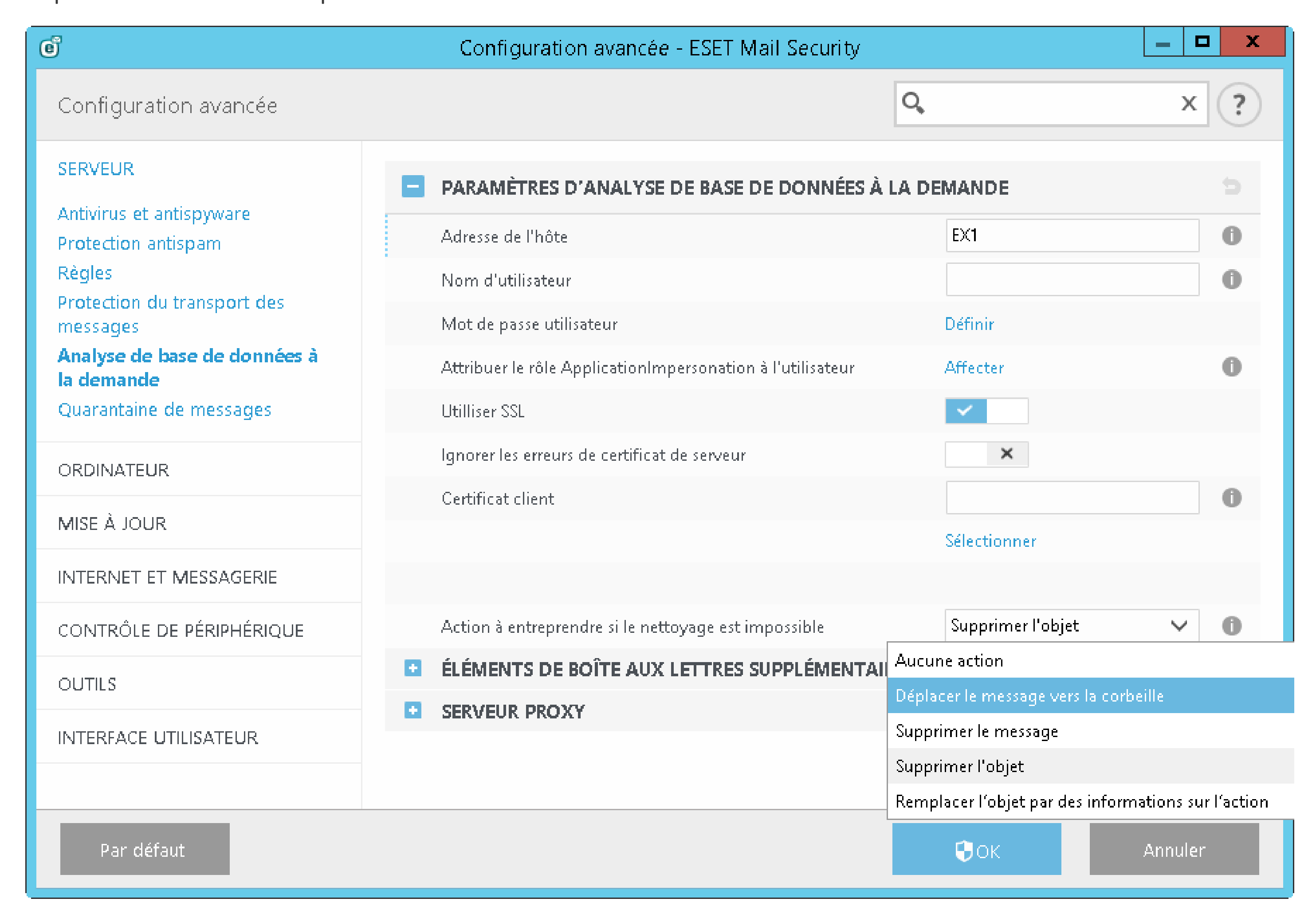
Attribuer le rôle ApplicationImpersonation à l'utilisateur : cliquez sur **Attribuer** pour attribuer automatiquement le

rôle ApplicationImpersonation à l'utilisateur sélectionné.

Utiliser SSL : cette option doit être activée si les services Web Exchange sont définis sur **Exiger SSL** dans IIS. Si SSL est activé, le certificat Exchange Server doit être importé dans le système avec ESET Mail Security (si les rôles Exchange Server se trouvent sur des serveurs différents). Les paramètres des services Web Exchange figurent dans IIS, dans *Sites/Default web site/EWS/SSL Settings*.

i **REMARQUE** : désactivez l'option **Utiliser SSL** uniquement si les services Web Exchange sont configurés pour ne pas exiger SSL dans IIS.

Certificat de client : ne doit être défini que lorsque les services Web Exchange requièrent le certificat de client. L'option **Sélectionner** vous permet de sélectionner les certificats.



Action à entreprendre si le nettoyage n'est pas possible : ce champ d'action permet de **bloquer** le contenu infecté.

Aucune action : aucune action à entreprendre sur le contenu infecté du message.
Déplacer le message vers la corbeille : cette action n'est pas prise en charge pour les éléments du dossier public. Vous pouvez utiliser l'action **Supprimer l'objet** à la place.
Supprimer l'objet : supprime le contenu infecté du message.
Supprimer le message : supprime l'intégralité du message, y compris son contenu infecté.
Remplacer l'objet par des informations sur l'action : supprime un objet et ajoute des informations sur l'action entreprise sur cet objet.

5.1.8.1 Éléments de boîte aux lettres supplémentaires

Les paramètres de l'analyseur de base de données à la demande permettent d'activer ou de désactiver l'analyse d'autres types d'élément de boîte aux lettres :

- Analyser le calendrier
- Analyser les tâches
- Analyser les contacts
- Analyser le journal

REMARQUE : si vous rencontrez des problèmes de performances, vous pouvez désactiver l'analyse de ces éléments. Les analyses durent plus longtemps lorsque ces éléments sont activés.

5.1.8.2 Serveur proxy

Si vous utilisez un serveur proxy entre le serveur Exchange Server avec le rôle de serveur d'accès au client et le serveur Exchange Server sur lequel ESET Mail Security est installé, indiquez les paramètres du serveur proxy. Ces paramètres sont obligatoires, car ESET Mail Security se connecte à l'API des services Web via HTTP/HTTPS. Si vous ne les indiquez pas, l'analyse de base de données à la demande ne fonctionnera pas.

Serveur proxy : saisissez l'adresse IP ou le nom du serveur proxy utilisé.

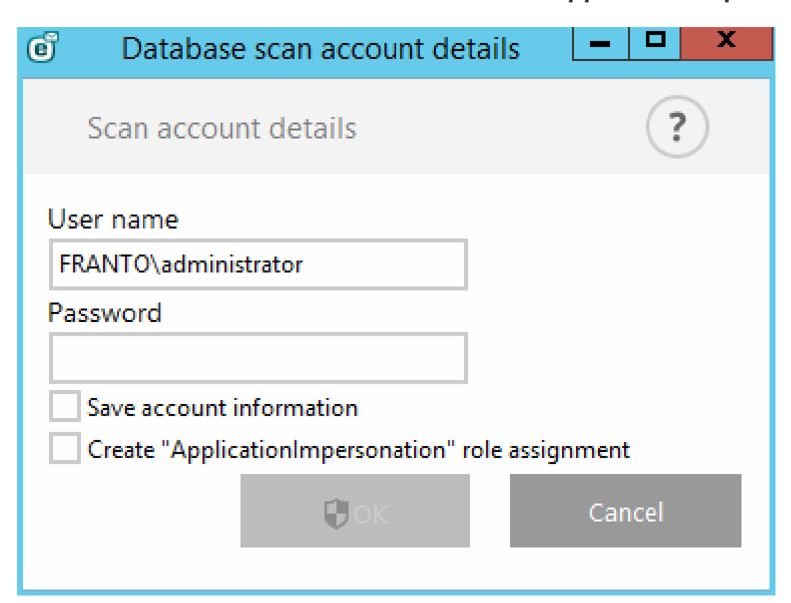
Port : saisissez le numéro de port du serveur proxy.

Nom d'utilisateur, mot de passe : saisissez les informations d'identification si le serveur proxy nécessite une authentification.

5.1.8.3 Détails du compte d'analyse de base de données

Cette boîte de dialogue s'affiche si vous n'avez pas indiqué un nom d'utilisateur ni un mot de passe pour l'**analyse de base de données** dans **Configuration avancée**. Indiquez les informations d'identification de l'utilisateur ayant accès aux services Web Exchange dans cette fenêtre indépendante, puis cliquez sur **OK**. Vous pouvez également accéder à **Configuration avancée** en appuyant sur **F5** et atteindre **Serveur** > Analyse de base de données à la demande. Tapez un **nom d'utilisateur**, cliquez sur **Définir**, tapez un mot de passe, puis cliquez sur OK.

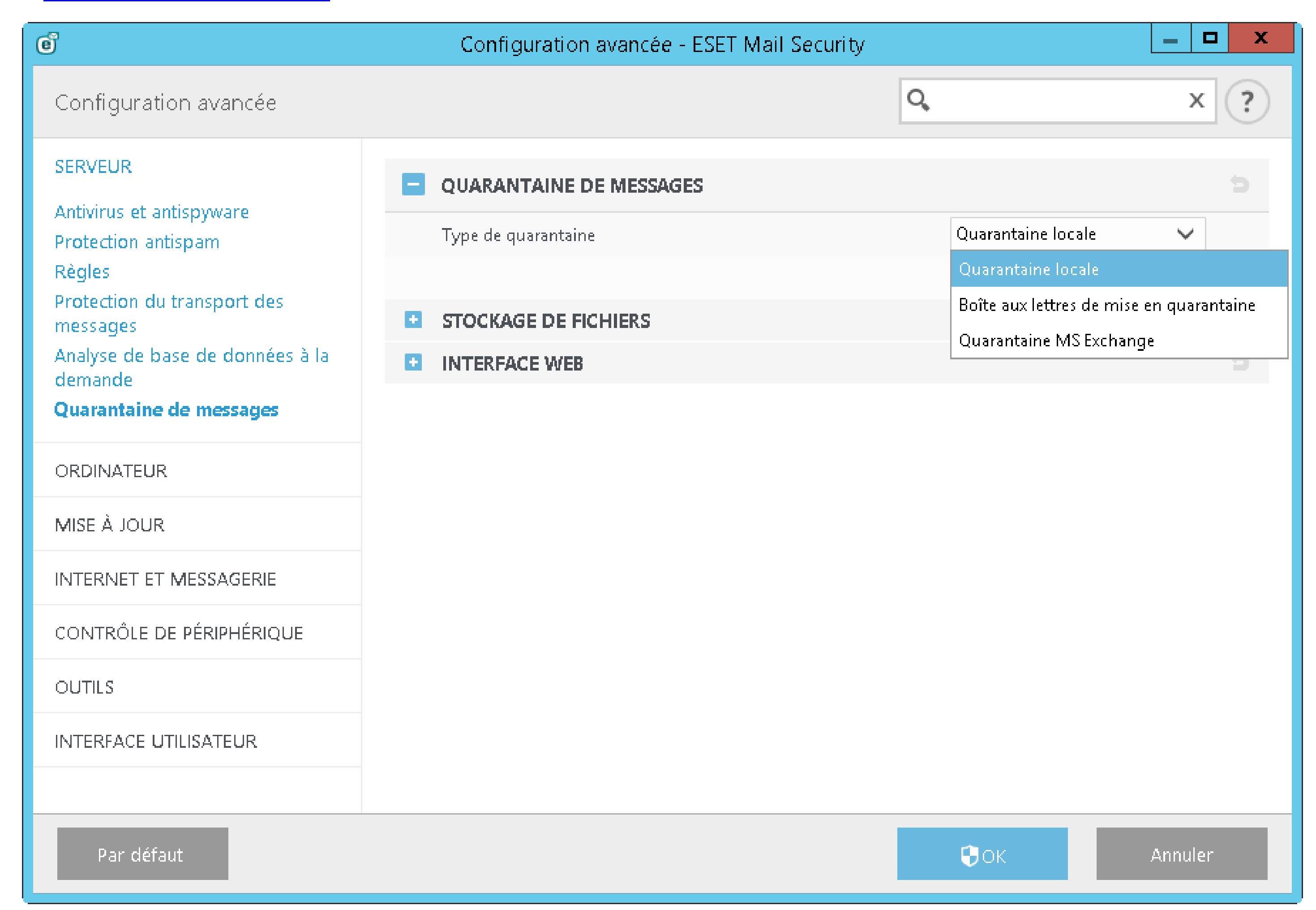
- Vous pouvez sélectionner **Enregistrer les informations du compte** pour enregistrer les paramètres du compte afin de ne pas avoir à les taper chaque fois que vous exécutez une analyse de base de données à la demande.
- Si un compte d'utilisateur ne dispose pas d'un accès adéquat aux services Web Exchange, vous pouvez sélectionner **Créer l'attribution du rôle « ApplicationImpersonation »** pour attribuer ce rôle à un compte.



5.1.9 Quarantaine de messages

Le gestionnaire de quarantaine de messages est disponible pour les trois types de quarantaine :

- Quarantaine locale
- Boîte aux lettres de quarantaine
- Quarantaine MS Exchange



Vous pouvez afficher le contenu de la quarantaine de messages dans le gestionnaire de quarantaine de messages pour tous les types de quarantaine. La quarantaine locale peut être en outre affichée dans l'interface Web Quarantaine de messages.

5.1.9.1 Quarantaine locale

La quarantaine locale utilise le système de fichiers local pour stocker les messages électroniques mis en quarantaine et une base de données SQLite en tant qu'index. Le fichier de base de données et les fichiers des messages électroniques mis en quarantaine stockés sont chiffrés pour des raisons de sécurité. Ces fichiers figurent dans `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (dans Windows Server 2008 et 2012) ou `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (dans Windows Server 2003).

Fonctionnalités de la quarantaine locale :

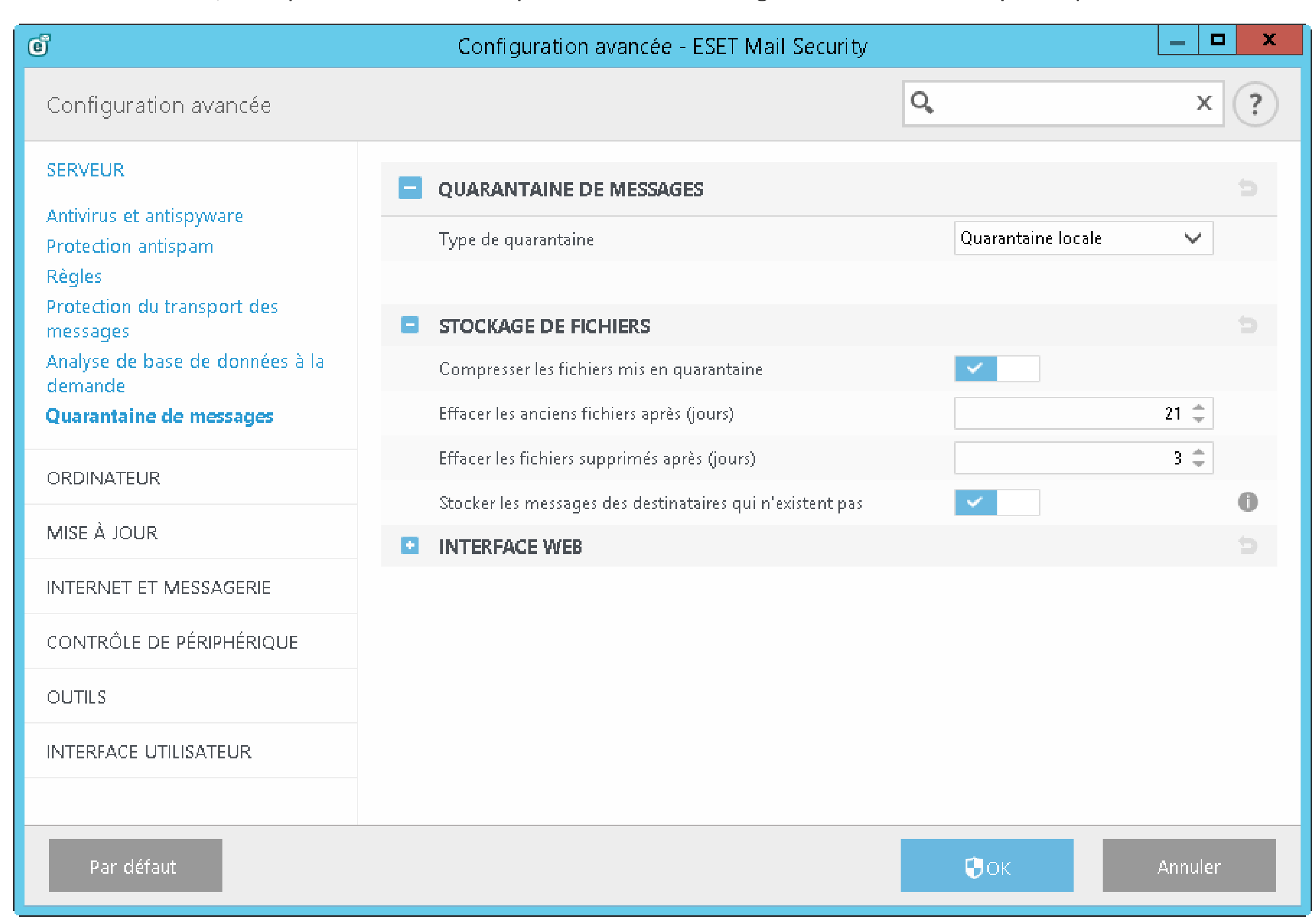
- Chiffrement et compression des fichiers des messages électroniques mis en quarantaine stockés.
- Les fichiers des messages électroniques mis en quarantaine supprimés de la fenêtre de quarantaine (au terme de 21 jours par défaut) sont toujours stockés dans un système de fichiers (jusqu'à ce que la suppression automatique ait lieu après un nombre spécifié de jours).
- Suppression automatique des anciens fichiers de messages électroniques (au terme de 3 jours par défaut). Pour plus d'informations, consultez les paramètres de stockage des fichiers.
- Vous pouvez restaurer les fichiers des messages électroniques mis en quarantaine supprimés à l'aide d'eShell (à

condition qu'ils n'aient pas encore été supprimés du système de fichiers).

Vous pouvez inspecter les messages électroniques mis en quarantaine et décider de les **supprimer** ou de les **libérer**. Pour afficher et gérer de manière locale les messages électroniques mis en quarantaine, vous pouvez utiliser le gestionnaire de quarantaine de messages à partir de l'interface utilisateur graphique principale ou l'interface Web Quarantaine de messages.

5.1.9.1.1 Stockage de fichiers

Dans cette section, vous pouvez modifier les paramètres du stockage des fichiers utilisé par la quarantaine locale.



Compresser les fichiers mis en quarantaine : les fichiers mis en quarantaine compressés occupent moins d'espace disque. Si vous ne souhaitez pas compresser les fichiers, utilisez le commutateur pour désactiver la compression.

Effacer les anciens fichiers après (jours) : lorsque les messages atteignent le nombre de jours spécifié, ils sont supprimés de la fenêtre de quarantaine. Toutefois, les fichiers ne sont pas supprimés du disque pendant le nombre de jours spécifié dans **Effacer les fichiers supprimés après (jours)**. Comme les fichiers ne sont pas supprimés du système de fichiers, il est possible de les récupérer à l'aide d'eShell.

Effacer les fichiers supprimés après (jours) : supprime les fichiers du disque après le nombre de jours spécifié. Aucune récupération n'est possible après la suppression des fichiers (à moins qu'une solution de sauvegarde du système ne soit en place).

Stocker les messages des destinataires qui n'existent pas : en règle générale, les messages indésirables sont envoyés à des destinataires aléatoires d'un domaine dans l'espoir d'accéder à un destinataire existant. Les messages envoyés aux utilisateurs qui n'existent pas dans Active Directory sont stockés par défaut dans la quarantaine locale. Vous pouvez toutefois désactiver cette option pour que les messages des destinataires qui n'existent pas ne soient pas stockés. Ainsi, la quarantaine locale ne sera pas encombrée par des messages indésirables de ce type. Cela permet également d'économiser de l'espace disque.

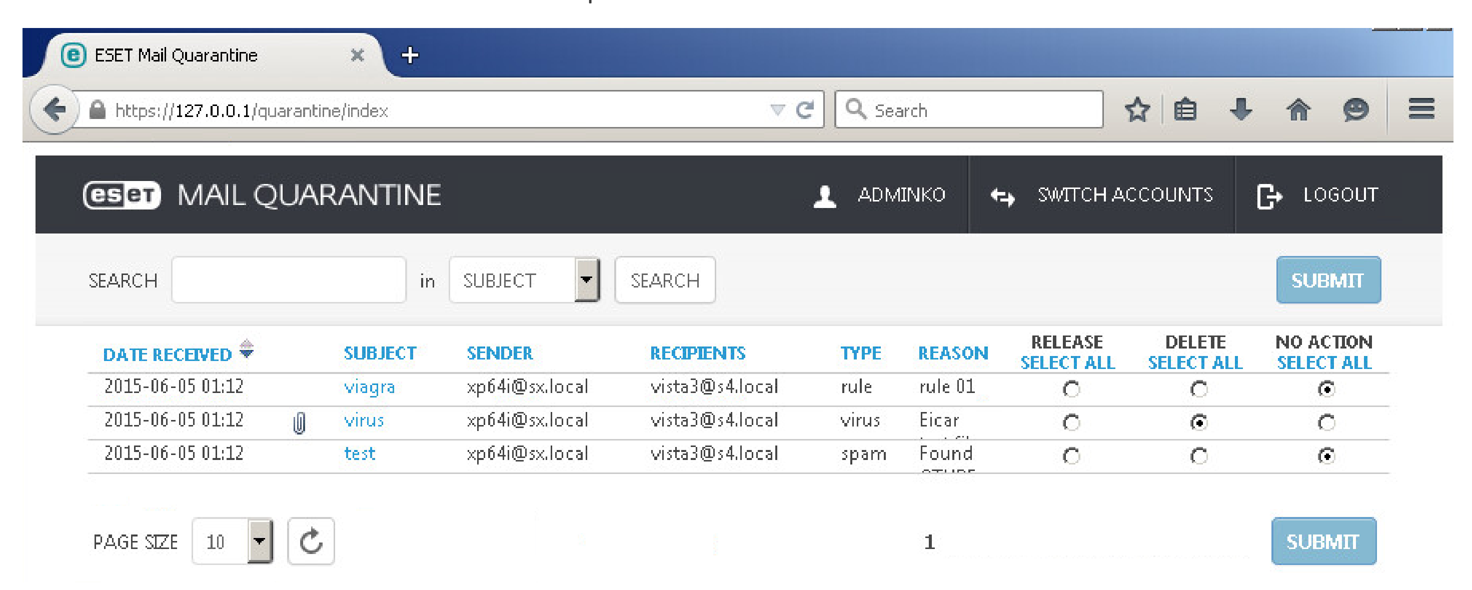
5.1.9.1.2 Interface Web

L'interface Web Quarantaine de messages est une solution que vous pouvez utiliser à la place du gestionnaire de quarantaine de messages. Elle n'est toutefois disponible que pour la quarantaine locale.

REMARQUE : l'interface Web Quarantaine de messages n'est pas disponible sur un serveur avec le rôle serveur de transport Edge, car Active Directory n'est pas accessible pour l'authentification.

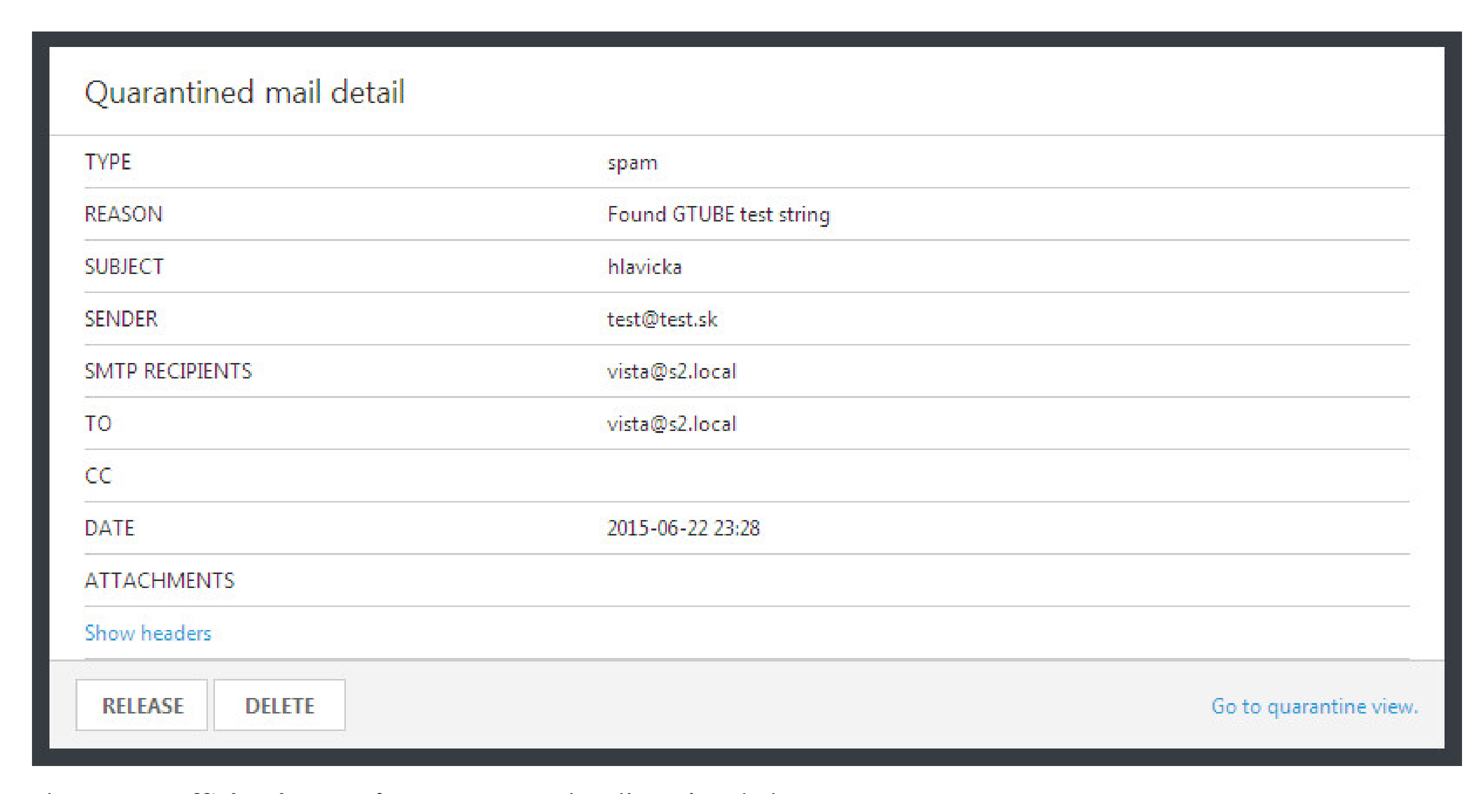
L'interface Web Quarantaine de messages permet d'afficher l'état de la quarantaine des messages. Elle permet également de gérer les objets des messages électroniques mis en quarantaine. Cette interface Web est accessible par le biais des liens contenus dans les rapports de mise en quarantaine ou en saisissant une URL dans votre navigateur Web. Pour accéder à l'interface Web Quarantaine de messages, vous devez vous authentifier à l'aide des informations d'identification du domaine. Internet Explorer effectue automatiquement l'authentification pour un utilisateur du domaine : le certificat de la page Web doit être valide, la connexion automatique doit être activée dans Internet Explorer et vous devez ajouter le site Web Quarantaine de messages aux sites de l'intranet local.

Le commutateur **Activer l'interface Web** vous permet d'activer ou de désactiver l'interface Web.



Libérer : libère le message électronique pour le ou les destinataires d'origine à l'aide du répertoire de lecture et le supprime de la quarantaine. Cliquez sur **Soumettre** pour confirmer l'action.
Supprimer : supprime l'élément de la quarantaine. Cliquez sur **Soumettre** pour confirmer l'action.

Lorsque vous cliquez sur **Objet**, une fenêtre indépendante s'ouvre. Elle contient des détails sur le message électronique mis en quarantaine tels que le **type**, le **motif**, l'**expéditeur**, la **date**, les **pièces jointes**, etc.



Cliquez sur **Afficher les en-têtes** pour consulter l'en-tête de la mise en quarantaine.

Quarantined mail detail

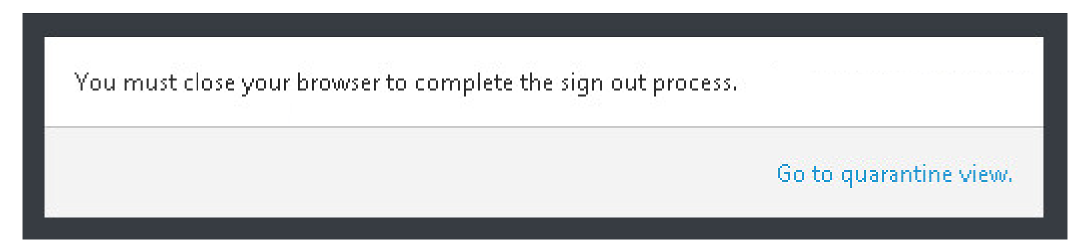
TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28
ATTACHMENTS	

Received: from win2k3r2x64-ss4 ([10.1.117.232]) by win2k3sp2x86ss1.s2.local with Microsoft SMTPSVC(6.0.3790.4675);
Mon, 22 Jun 2015 23:28:46 -0700
Received:
To: <vista@s2.local>
Subject:[SPAM] hlavicka
X-Originating-IP:
MIME-Version: 1.0
Content-Type: text/plain
Message-ID: <-974233353.8808@win2k8x64-EDGE.s1.local>
From:
Return-Path: <>
Date: Tue, 9 Nov 2010 22:12:48 -0800
X-MS-Exchange-Organization-OriginalArrivalTime: 10 Nov 2010 06:12:48.9975
(UTC)
X-MS-Exchange-Organization-AuthSource: win2k8x64-EDGE.s1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
Received-SPF: Fail (win2k8x64-EDGE.s1.local: domain of does not designate
10.1.117.225 as permitted sender) receiver=win2k8x64-EDGE.s1.local;

RELEASE DELETE Go to quarantine view.

Si vous le souhaitez, cliquez sur **Libérer** ou **Supprimer** pour exécuter une action sur un message électronique mis en quarantaine.

i **REMARQUE** : vous devez fermer la fenêtre de votre navigateur pour vous déconnecter complètement de l'interface Web Quarantaine de messages. Sinon, cliquez sur **Atteindre** dans la vue de quarantaine pour revenir à l'écran précédent.



Important : si vous rencontrez des problèmes pour accéder à l'interface Web Quarantaine de messages à partir de votre navigateur ou si l'erreur `Erreur HTTP 403.4 - Interdit` s'affiche, vérifiez quel type de quarantaine est sélectionné et assurez-vous que les options **Quarantaine locale** et **Activer l'interface Web** sont activées.

5.1.9.2 Boîte aux lettres de quarantaine et quarantaine MS Exchange

Si vous choisissez de ne pas utiliser l'option Quarantaine locale, vous disposez de deux autres options : **Boîte aux lettres de quarantaine** et **Quarantaine MS Exchange**. Quelle que soit l'option choisie, vous devez créer un utilisateur dédié avec une boîte aux lettres (par exemple quarantaine principale@entreprise.com) qui sera utilisée pour stocker les messages électroniques mis en quarantaine. Cet utilisateur et la boîte aux lettres seront également utilisés par le gestionnaire de quarantaine de messages pour afficher et gérer les éléments en quarantaine. Vous devez indiquer les détails du compte de cet utilisateur dans les Paramètres du gestionnaire de la mise en quarantaine.

Important : il n'est pas recommandé d'utiliser le compte d'utilisateur Administrateur en tant que boîte aux lettres de quarantaine.

REMARQUE : l'option **Quarantaine MS Exchange** n'est pas disponible pour Microsoft Exchange 2003. Seules les options **Quarantaine locale** et **Boîte aux lettres de quarantaine** le sont.

- Lorsque vous sélectionnez **Quarantaine MS Exchange**, ESET Mail Security utilise le **système de quarantaine Microsoft Exchange** (cela s'applique à Microsoft Exchange Server 2007 et version ultérieure). Dans ce cas, le mécanisme interne Exchange stocke les messages potentiellement infectés et le courrier potentiellement indésirable.

REMARQUE : par défaut, cette quarantaine interne n'est pas activée dans Exchange. Si vous souhaitez l'activer, vous devez ouvrir l'environnement de ligne de commande Exchange Management Shell et entrer la commande suivante (remplacez `nom@domaine.com` par l'adresse actuelle de la boîte aux lettres dédiée) :

```
Set-ContentFilterConfig -QuarantineMailbox nom@domaine.com
```

- Lorsque vous sélectionnez **Boîte aux lettres de quarantaine**, vous devez indiquer l'adresse de quarantaine des messages (par exemple quarantaine principale@entreprise.com).

5.1.9.2.1 Paramètres du gestionnaire de la mise en quarantaine

Adresse de l'hôte : apparaît automatiquement si le serveur Exchange Server avec le rôle de serveur d'accès au client est présent localement. Si le rôle de serveur d'accès au client n'est pas présent sur le serveur sur lequel ESET Mail Security est installé mais s'il peut être détecté dans Active Directory, l'adresse de l'hôte apparaît aussi automatiquement. Si elle n'apparaît pas, vous pouvez saisir manuellement le nom de l'hôte. La détection automatique ne fonctionne pas avec le rôle de serveur de transport Edge.

REMARQUE : l'adresse IP n'est pas prise en charge. Vous devez utiliser le nom de l'hôte du serveur d'accès au client.

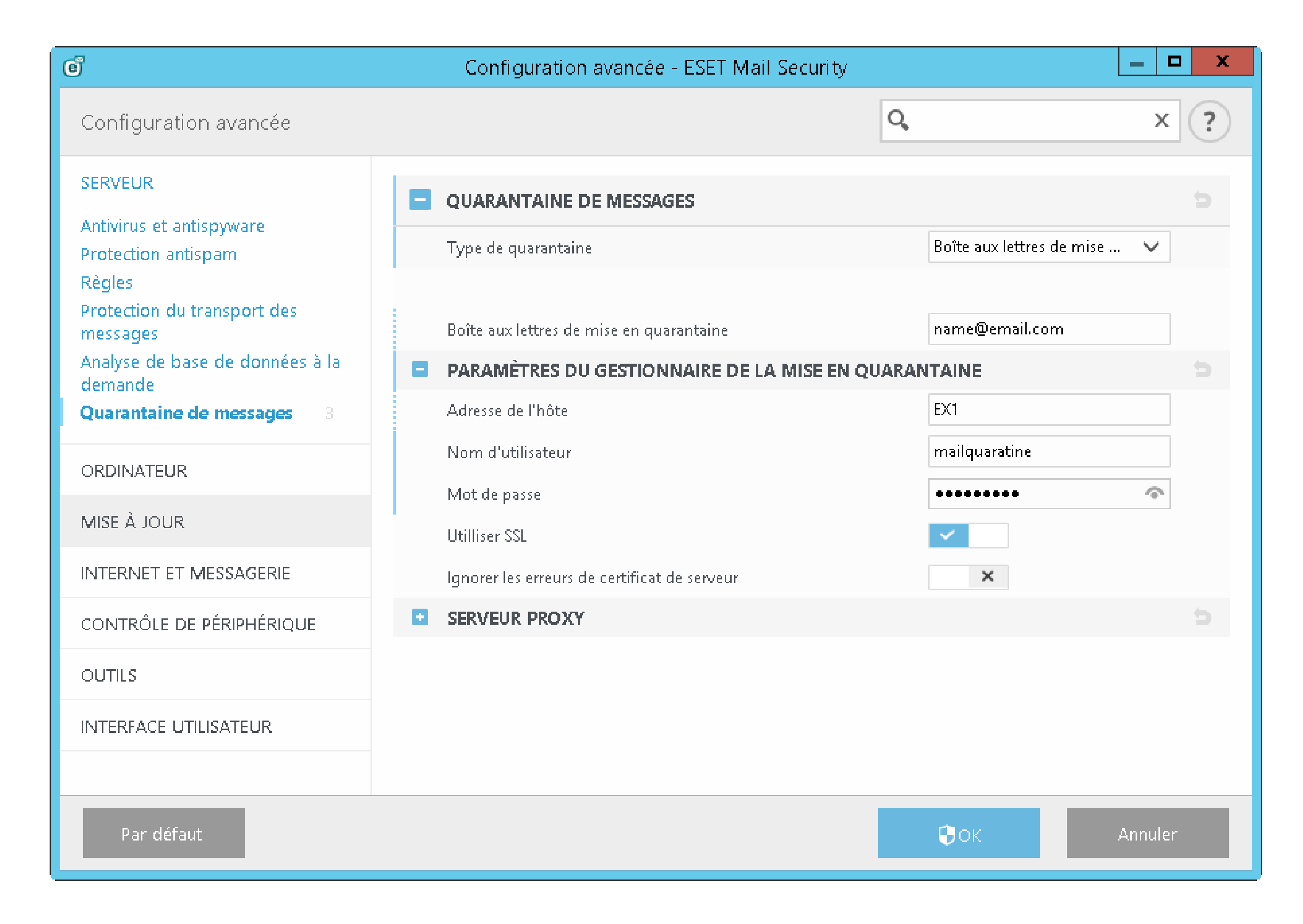
Nom d'utilisateur : compte d'utilisateur de quarantaine dédié que vous avez créé pour stocker les messages mis en quarantaine (ou compte ayant accès à cette boîte aux lettres via la délégation d'accès). Pour le rôle de serveur de transport Edge qui n'appartient pas au domaine, il est nécessaire d'utiliser l'adresse électronique complète (quarantaine_principale@entreprise.com, par exemple).

Mot de passe : saisissez le mot de passe de votre compte de quarantaine.

Utiliser SSL : cette option doit être activée si les services Web Exchange sont définis sur **Exiger SSL** dans IIS. Si SSL est activé, le certificat Exchange Server doit être importé dans le système avec ESET Mail Security (si les rôles Exchange Server se trouvent sur des serveurs différents). Les paramètres des services Web Exchange figurent dans IIS, dans *Sites/Default web site/EWS/SSL Settings*.

REMARQUE : désactivez l'option **Utiliser SSL** uniquement si les services Web Exchange sont configurés pour ne pas exiger SSL dans IIS.

Ignorer les erreurs de certificat de serveur : ignore les états suivants : signé automatiquement, nom incorrect dans le certificat, utilisation incorrecte, expiré.



5.1.9.2.2 Serveur proxy

Si vous utilisez un serveur proxy entre le serveur Exchange Server avec le rôle de serveur d'accès au client et le serveur Exchange Server sur lequel ESET Mail Security est installé, indiquez les paramètres du serveur proxy. Ces paramètres sont obligatoires, car ESET Mail Security se connecte à l'API des services Web via HTTP/HTTPS. Si vous ne les indiquez pas, la boîte aux lettre de quarantaine et la quarantaine MS Exchange ne fonctionneront pas.

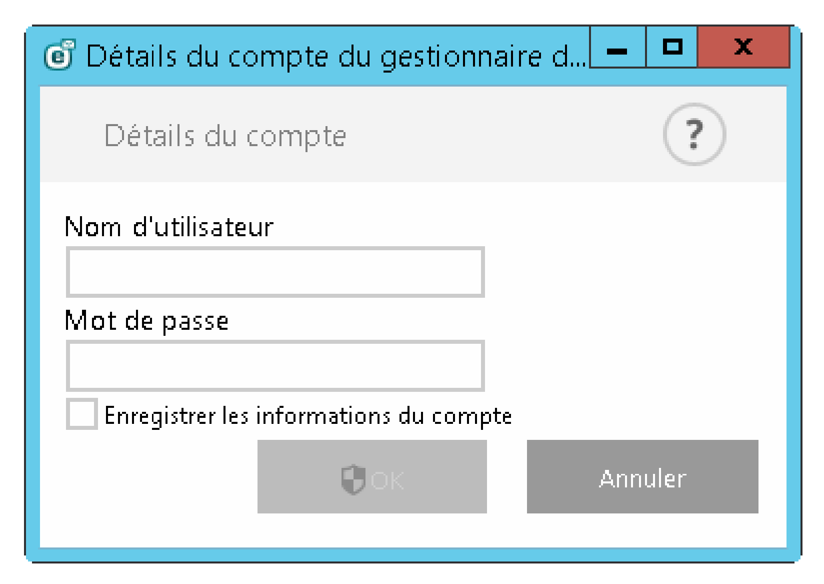
Serveur proxy : saisissez l'adresse IP ou le nom du serveur proxy utilisé.

Port : saisissez le numéro de port du serveur proxy.

Nom d'utilisateur, mot de passe : saisissez les informations d'identification si le serveur proxy nécessite une authentification.

5.1.9.3 Détails du compte du gestionnaire de mise en quarantaine

Cette boîte de dialogue s'affiche si vous n'avez pas configuré de compte pour **Détails du compte du gestionnaire de mise en quarantaine**. Indiquez les informations d'identification d'un utilisateur disposant d'un accès à la boîte aux lettres de **quarantaine**, puis cliquez sur **OK**. Vous pouvez également appuyer sur F5 pour accéder à **Configuration avancée** et atteindre **Serveur** > **Quarantaine des messages** > Paramètres du gestionnaire de la mise en quarantaine. Saisissez le **nom d'utilisateur** et le **mot de passe** de la boîte aux lettres de quarantaine.



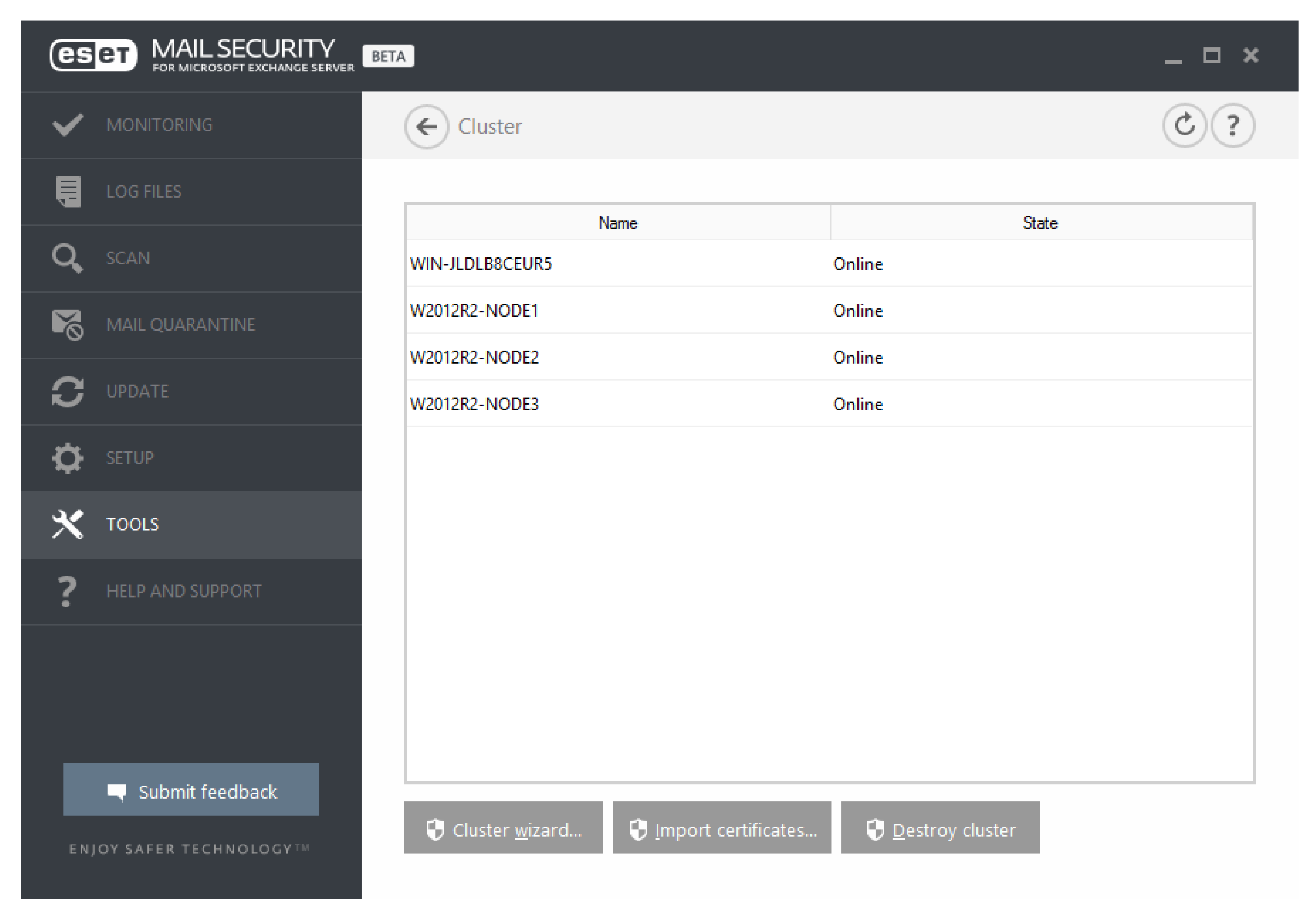
Vous pouvez sélectionner **Enregistrer les informations du compte** pour enregistrer les paramètres du compte pour une utilisation ultérieure lors de l'accès au gestionnaire de mise en quarantaine.

5.1.10 Cluster

ESET Cluster est une infrastructure de communication P2P de la gamme des produits ESET pour Microsoft Windows Server.

Cette infrastructure permet aux produits serveur d'ESET de communiquer les uns avec les autres et d'échanger des données (configuration et notifications, par exemple), ainsi que de synchroniser les données nécessaires pour le fonctionnement correct d'un groupe d'instances de produit. Un exemple de ce type de groupe peut être un groupe de nœuds dans un cluster de basculement Windows ou un cluster d'équilibrage de la charge réseau doté d'un produit ESET et dans lequel la configuration du produit doit être identique dans l'ensemble du cluster. ESET Cluster assure cette cohérence entre les instances.

Vous pouvez accéder à la page d'état ESET Cluster dans le menu principal en cliquant sur **Outils** > **Cluster**. Lorsque ce produit est configuré correctement, la page d'état a cet aspect :



Pour configurer ESET Cluster, cliquez sur **Assistant Cluster...**. Pour plus d'informations sur la configuration d'ESET Cluster à l'aide de l'assistant, cliquez ici.

Lors de la configuration d'ESET Cluster, vous pouvez ajouter des nœuds de deux manières : automatiquement à l'aide du cluster de basculement Windows/d'équilibrage de la charge réseau existant ou manuellement en recherchant des ordinateurs se trouvant dans un domaine ou un groupe de travail.

Détection automatique - Détecte automatiquement les nœuds déjà membres d'un cluster de basculement Windows/d'équilibrage de la charge réseau, puis les ajoute à ESET Cluster.
Parcourir - Vous pouvez ajouter manuellement des nœuds en saisissant les noms des serveurs (membres d'un même groupe de travail ou d'un même domaine).

REMARQUE : les serveurs ne doivent pas obligatoirement être membres d'un cluster de basculement Windows/d'équilibrage de la charge réseau pour utiliser la fonctionnalité ESET Cluster. Il n'est pas nécessaire que votre environnement comporte un cluster de basculement Windows/d'équilibrage de la charge réseau pour que vous puissiez utiliser ESET Cluster.

Une fois que vous avez ajouté des nœuds à ESET Cluster, l'étape suivante consiste à installer ESET Mail Security sur chaque nœud. Cette installation est effectuée automatiquement lors de la configuration d'ESET Cluster.

Informations d'identification nécessaires pour une installation à distance d'ESET Mail Security sur d'autres nœuds du cluster :

- Domaine : informations d'identification de l'administrateur du domaine
- Groupe de travail : vous devez veiller à ce que tous les nœuds utilisent les mêmes informations d'identification de compte d'administrateur local

Dans ESET Cluster, vous pouvez également utiliser une combinaison de nœuds automatiquement ajoutés en tant que membres d'un cluster de basculement Windows/d'équilibrage de la charge réseau existant et de nœuds manuellement ajoutés (à condition qu'ils se trouvent dans le même domaine).

REMARQUE : il n'est pas possible de combiner des nœuds de domaine et des nœuds de groupe de travail.

L'utilisation d'ESET Cluster exige également que l'option **Partage de fichiers et d'imprimantes** soit activée dans le Pare-feu Windows avant que l'installation d'ESET Mail Security soit poussée sur les nœuds d'ESET Cluster.

Vous pouvez démanteler ESET Cluster facilement en cliquant sur **Détruire le cluster**. Chaque nœud écrit alors un enregistrement sur la destruction d'ESET Cluster dans son journal des événements. Ensuite, toutes les règles du pare-feu ESET sont supprimées du Pare-feu Windows. Les anciens nœuds reviennent alors à leur état initial et peuvent être réutilisés dans un autre ESET Cluster, si nécessaire.

REMARQUE : la création d'ESET Clusters entre ESET Mail Security et ESET File Security pour Linux n'est pas pris en charge.

L'ajout de nouveaux nœuds à un ESET Cluster existant peut être effectué à tout moment en exécutant l'**Assistant Cluster** comme décrit plus haut et ici.

Consultez la section Cluster pour plus d'informations sur la configuration d'ESET Cluster.

5.1.10.1 Assistant Cluster - page 1

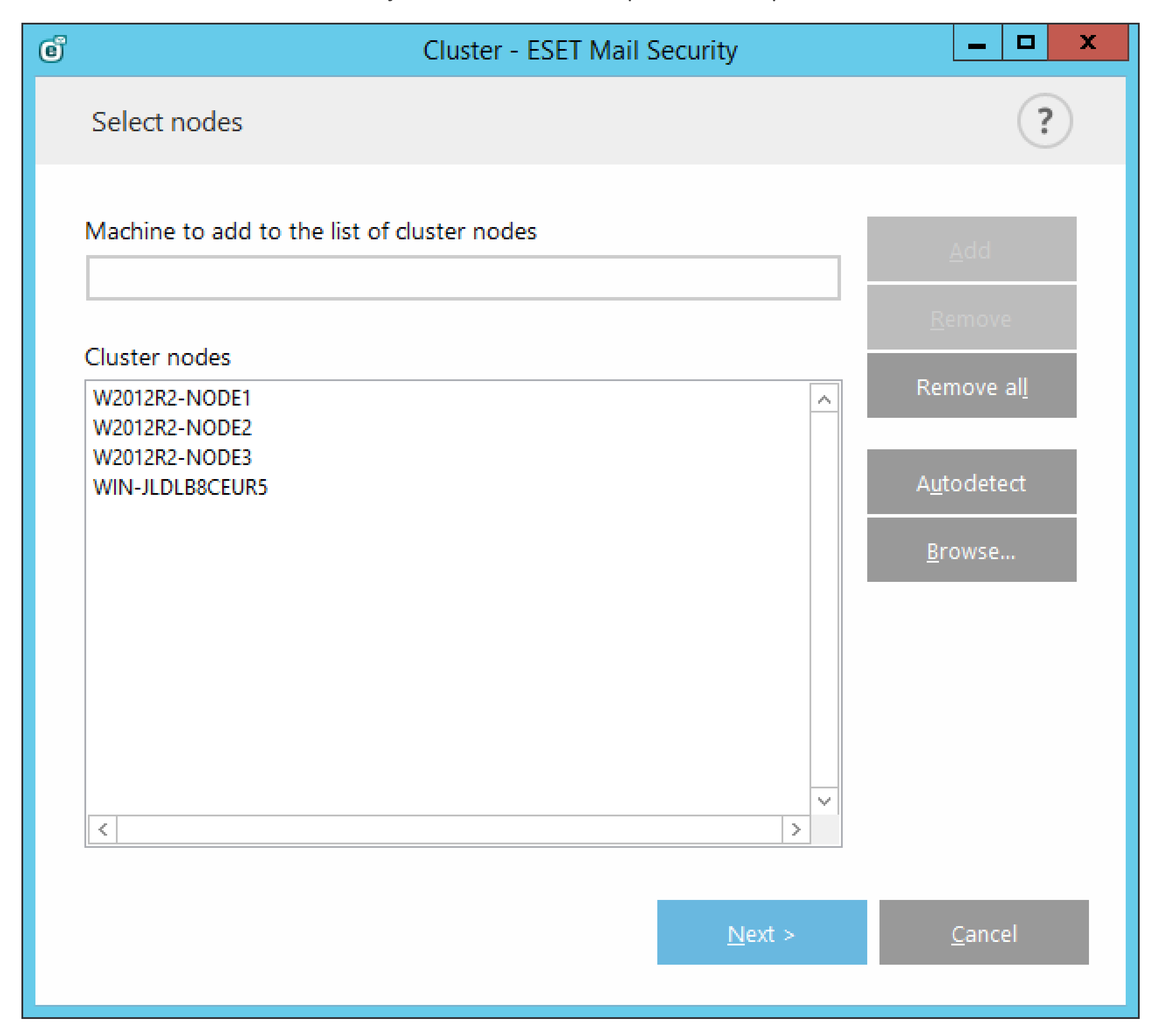
Lors de la configuration d'un ESET Cluster, la première étape consiste à ajouter des nœuds. Vous pouvez utiliser l'option **Détection automatique** ou la commande **Parcourir** pour ajouter des nœuds. Vous pouvez également saisir le nom du serveur dans la zone de texte, puis cliquer sur le bouton **Ajouter**.

L'option **Détection automatique** ajoute automatiquement les nœuds d'un cluster de basculement Windows/d'équilibrage de la charge réseau existant. Le serveur à partir duquel vous créez l'ESET Cluster doit être membre de ce cluster de basculement Windows/d'équilibrage de la charge réseau pour pouvoir ajouter automatiquement les nœuds. La fonctionnalité **Autoriser le contrôle à distance** doit être activée dans les propriétés du cluster d'équilibrage de la charge réseau afin qu'ESET Cluster puisse détecter correctement les nœuds. Une fois que vous obtenez la liste des nouveaux nœuds ajoutés, vous pouvez supprimer ceux que vous ne souhaitez pas pour ne conserver que des nœuds spécifiques dans l'ESET Cluster.

Cliquez sur **Parcourir** pour rechercher des ordinateurs et les sélectionner dans un domaine ou un groupe de travail. Cette méthode permet d'ajouter manuellement des nœuds à ESET Cluster.

Une autre méthode pour ajouter des nœuds consiste à saisir le nom d'hôte du serveur à ajouter, puis à cliquer sur **Ajouter**.

Nœuds de cluster sélectionnés à ajouter à ESET Cluster après avoir cliqué sur **Suivant** :



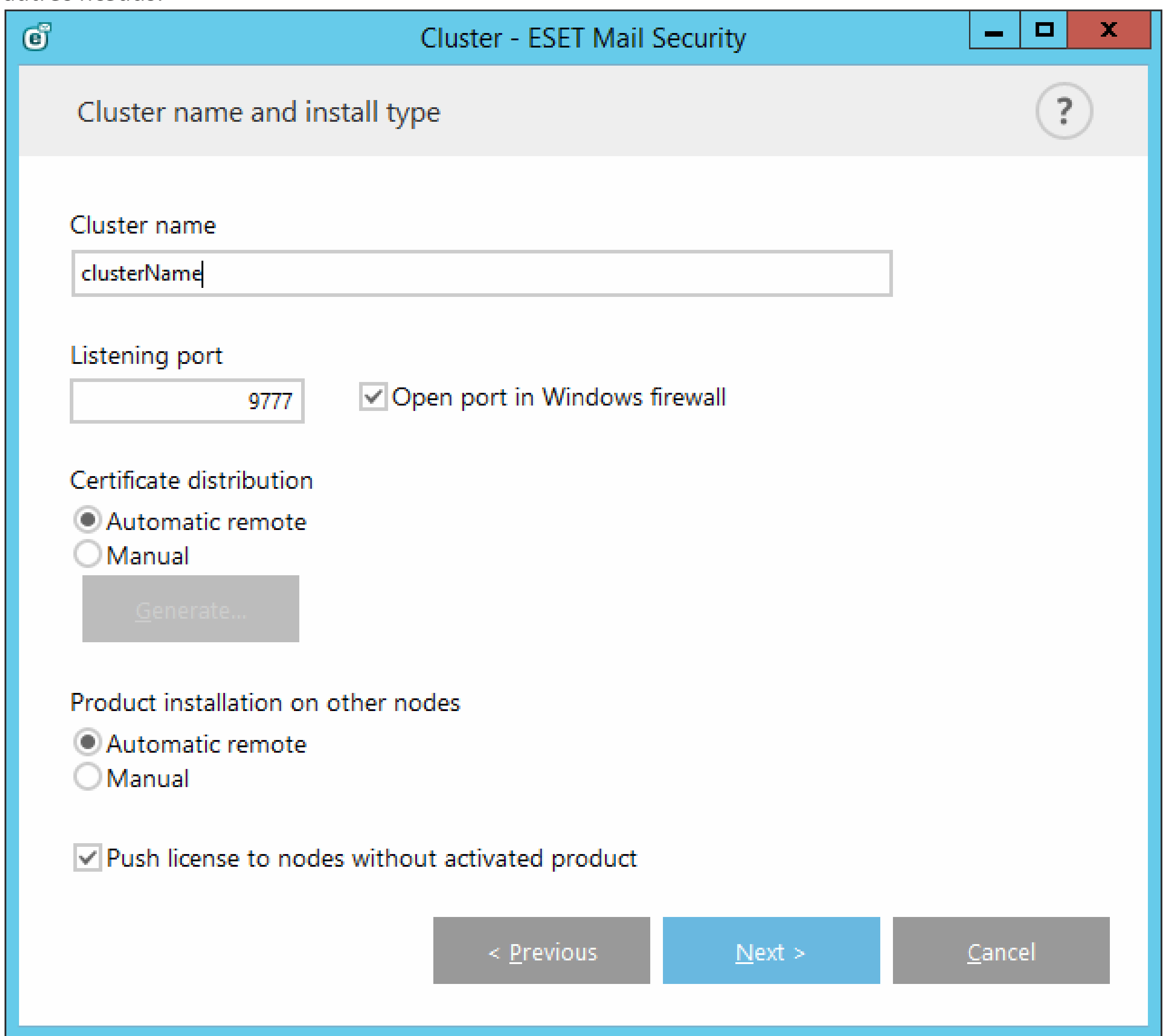
Pour modifier des **nœuds de cluster** dans la liste, sélectionnez le nœud que vous souhaitez supprimer, puis cliquez sur **Supprimer**. Pour effacer entièrement la liste, cliquez sur **Supprimer tout**.

Si vous disposez déjà d'un ESET Cluster, vous pouvez à tout moment y ajouter de nouveaux nœuds. La procédure est identique à celle décrite ci-dessus.

REMARQUE : tous les nœuds qui sont conservés dans la liste doivent être en ligne et accessibles. Par défaut, Localhost est ajouté aux nœuds du cluster.

5.1.10.2 Assistant Cluster - page 2

Définissez le nom d'un cluster, le mode de distribution des certificats et l'installation ou non du produit sur les autres nœuds.



Nom du cluster - Saisissez le nom du cluster.
Port d'écoute - Le port par défaut est 9777.
Ouvrir le port dans le Pare-feu Windows : lorsque cette case est cochée, une règle est créée dans le Pare-feu Windows.

Distribution de certificats :
Automatique à distance : le certificat est installé automatiquement.
Manuelle - Lorsque vous cliquez sur **Générer**, une fenêtre de navigation s'ouvre. Sélectionnez le dossier dans lequel stocker les certificats. Les certificats suivants sont créés : un certificat racine et un certificat pour chaque nœud, notamment pour celui (ordinateur local) à partir duquel vous configurez ESET Cluster. Vous pouvez ensuite choisir d'inscrire le certificat sur l'ordinateur local en cliquant sur **Oui**. Vous devrez importer ultérieurement les certificats manuellement, comme décrit ici.

Installation du produit sur les autres nœuds :
Automatique à distance - ESET Mail Security est installé automatiquement sur chaque nœud (à condition que l'architecture des systèmes d'exploitation soit identique).
Manuelle - Sélectionnez cette option si vous souhaitez installer manuellement ESET Mail Security (lorsque les architectures des systèmes d'exploitation sont différentes sur certains nœuds, par exemple).

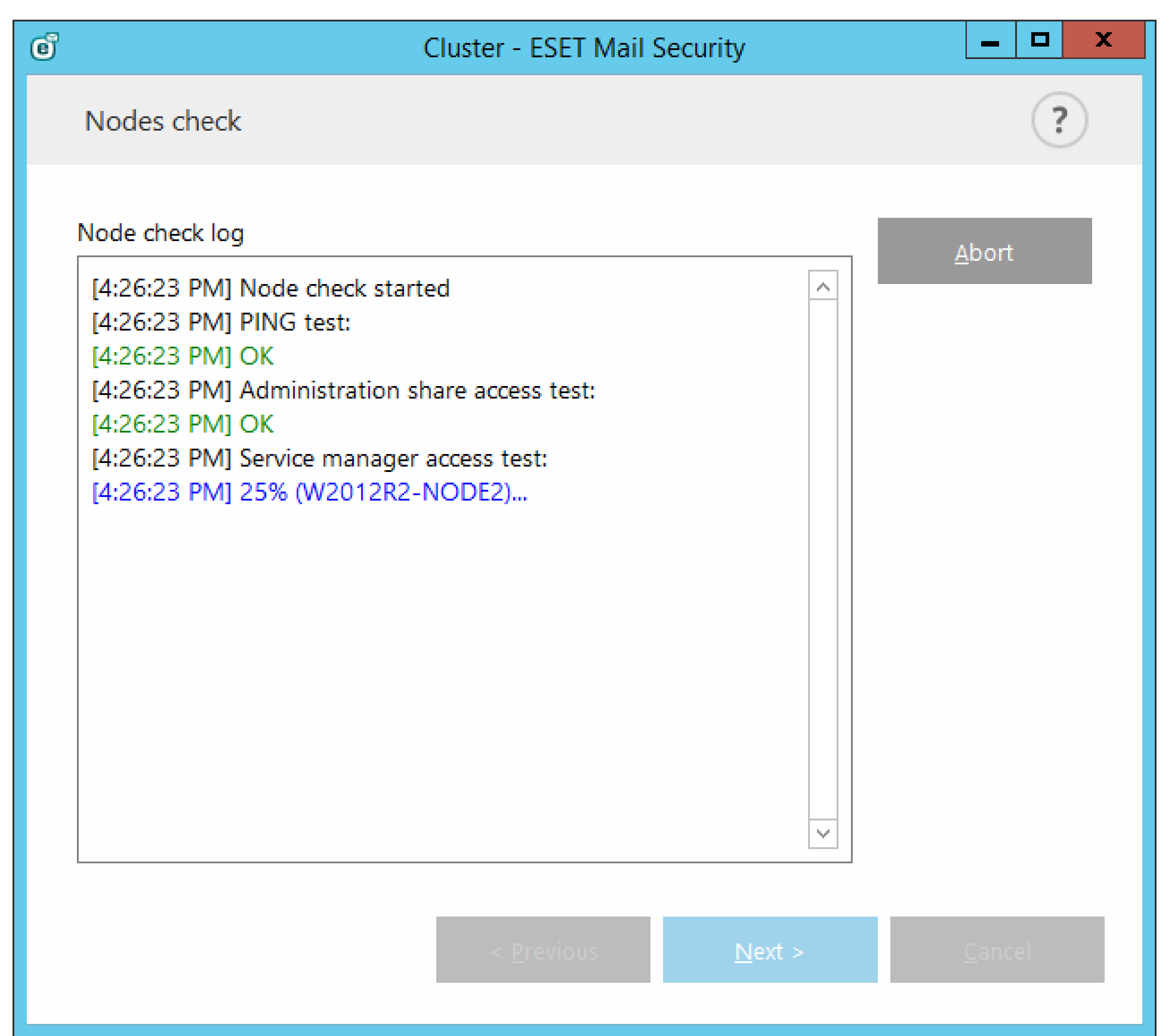
Transmettre la licence aux nœuds sans produit activé - Lorsque cette option est cochée, les nœuds activent ESET Mail Security.

REMARQUE : si vous souhaitez créer un ESET Cluster avec des architectures de système d'exploitation mixtes (32 et 64 bits), vous devez installer ESET Mail Security manuellement. Cela est détecté lors des étapes suivantes. Ces informations sont alors affichées dans la fenêtre de journal.

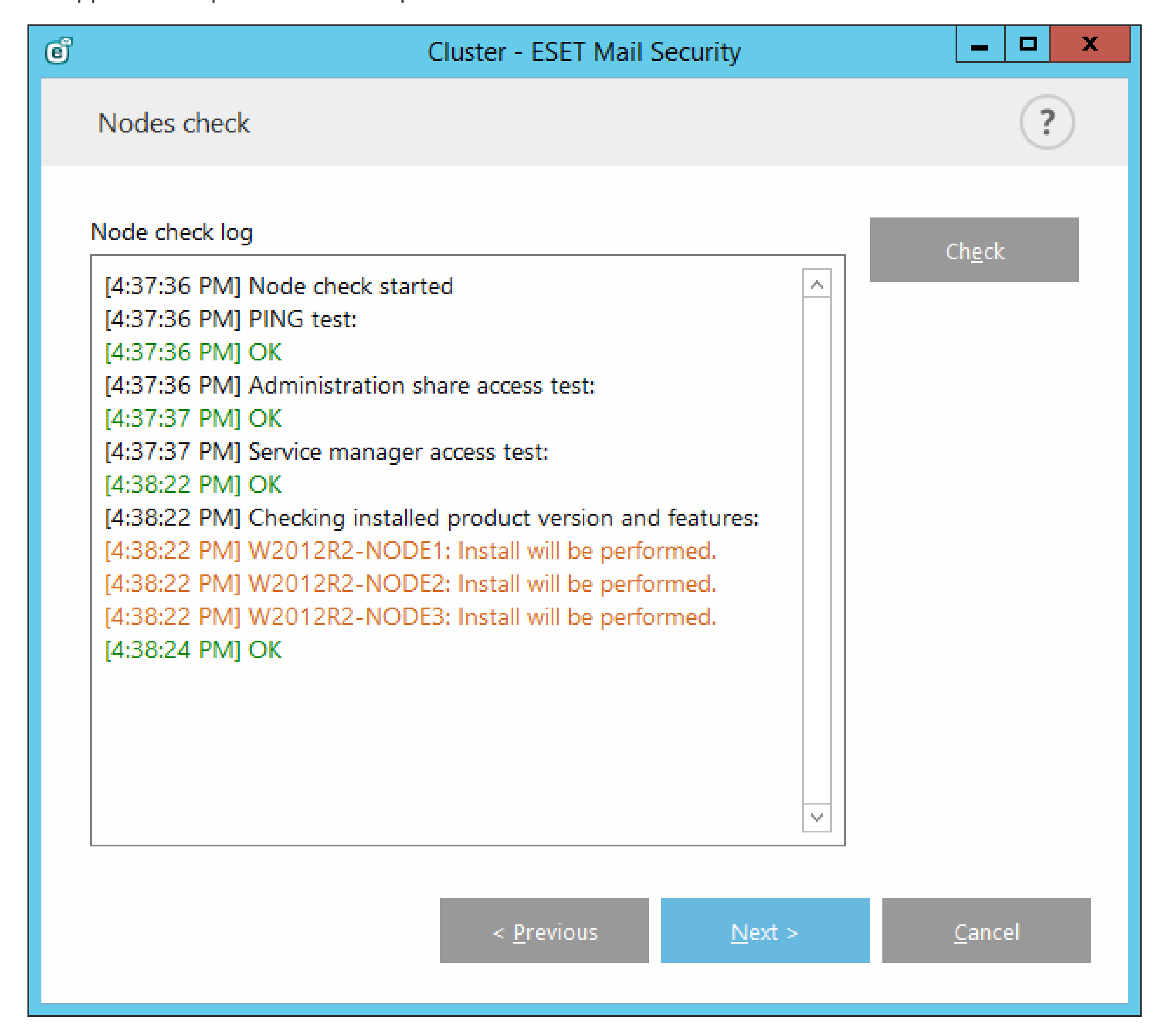
5.1.10.3 Assistant Cluster - page 3

Une fois les informations d'installation spécifiées, une vérification des nœuds est exécutée. Dans **Journal de vérification des nœuds**, les points suivants sont vérifiés :

- Tous les nœuds existants sont en ligne.
- Les nouveaux nœuds sont accessibles.
- Le nœud est en ligne.
- Le partage administratif est accessible.
- Une exécution à distance est possible.
- La version correcte du produit est installée ou aucun produit n'est signalé (uniquement si l'installation automatique est sélectionnée).
- Les nouveaux certificats sont présents.

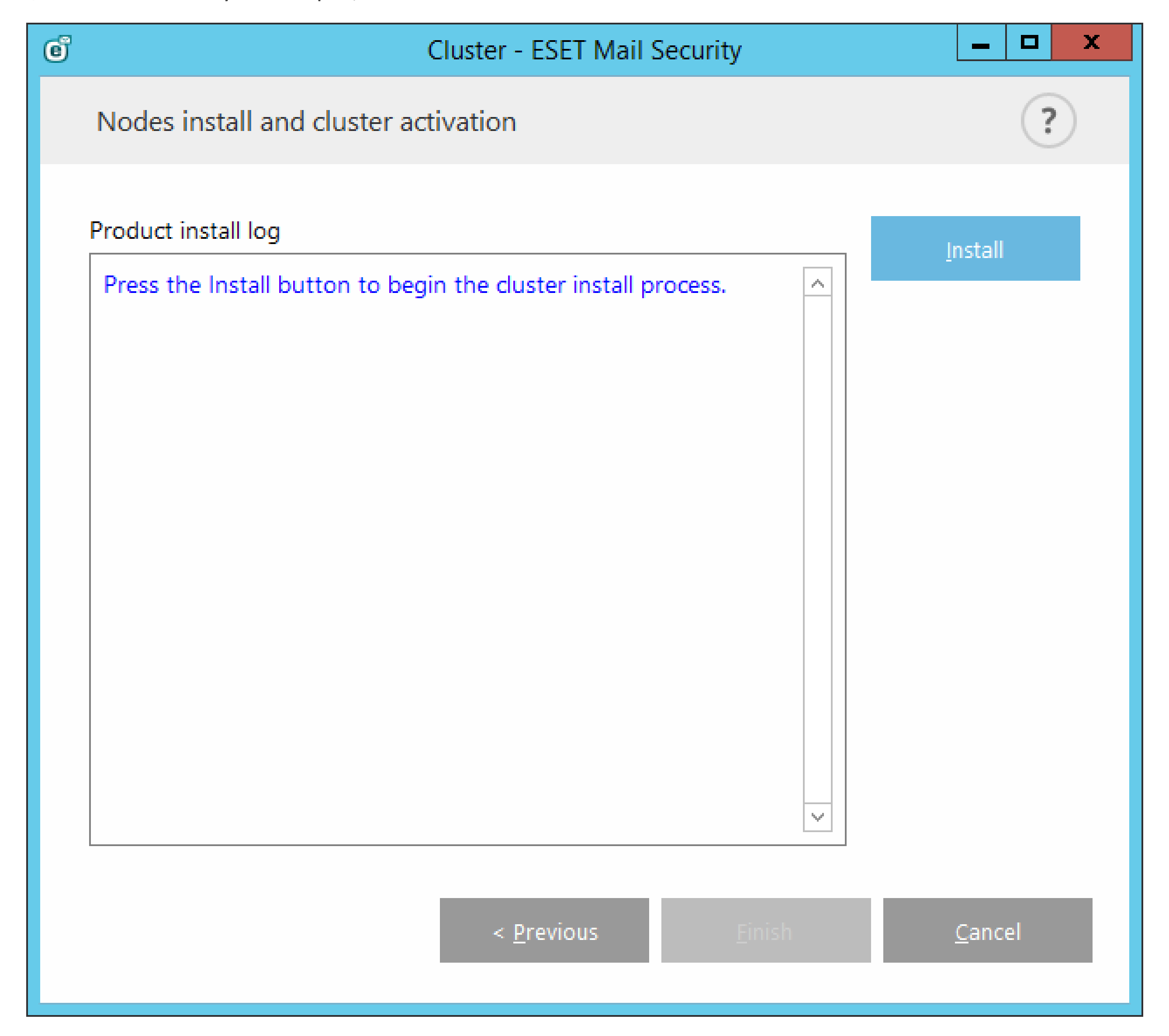


Le rapport est disponible une fois que la vérification des nœuds est terminée :



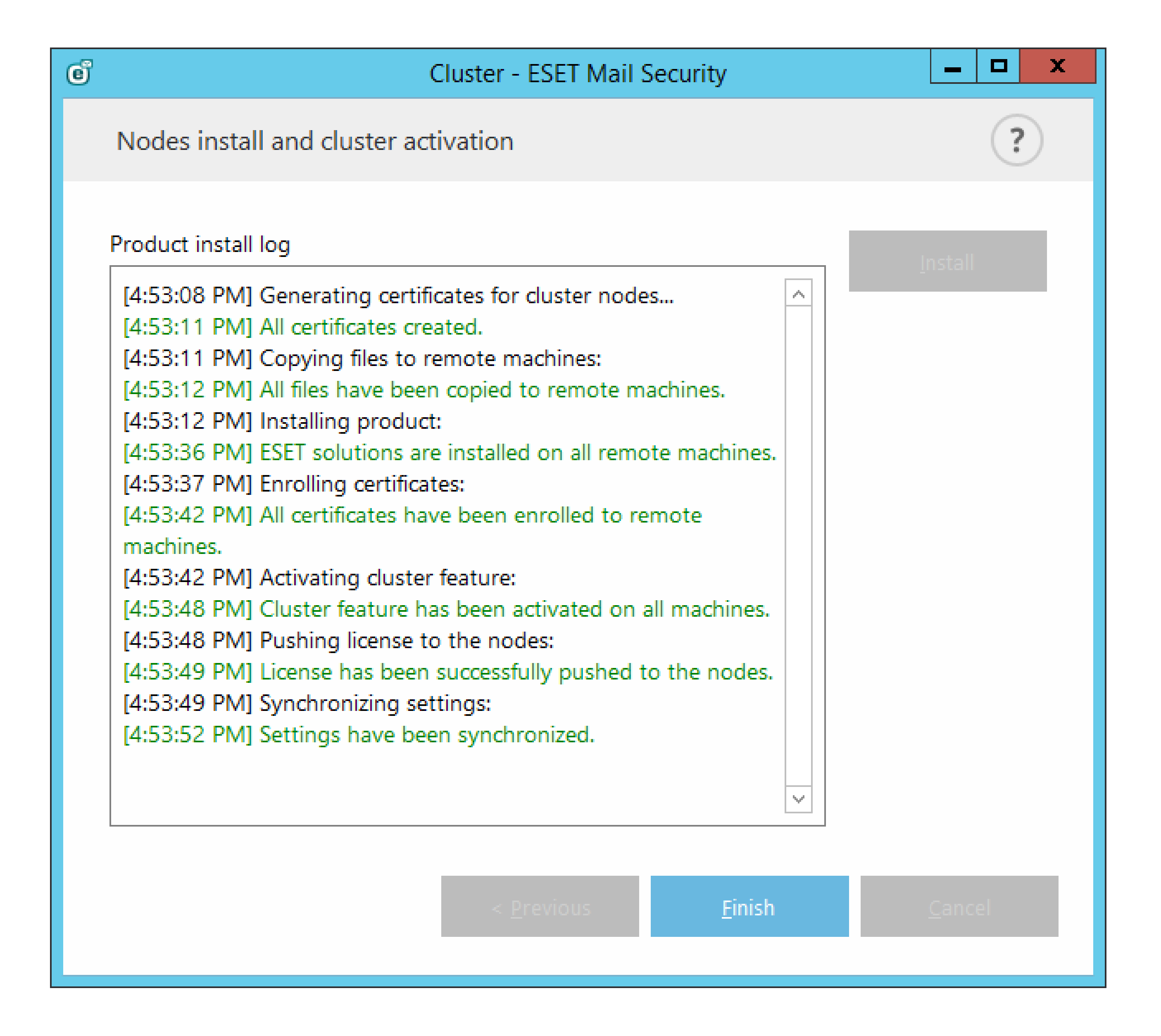
5.1.10.4 Assistant Cluster - page 4

Lorsque le produit doit être installé sur un ordinateur distant lors de l'initialisation d'ESET Cluster, le package d'installation recherche le programme d'installation dans le répertoire %ProgramData%\ESET\<Nom_produit>\Installer. S'il ne s'y trouve pas, l'utilisateur est invité à le rechercher.

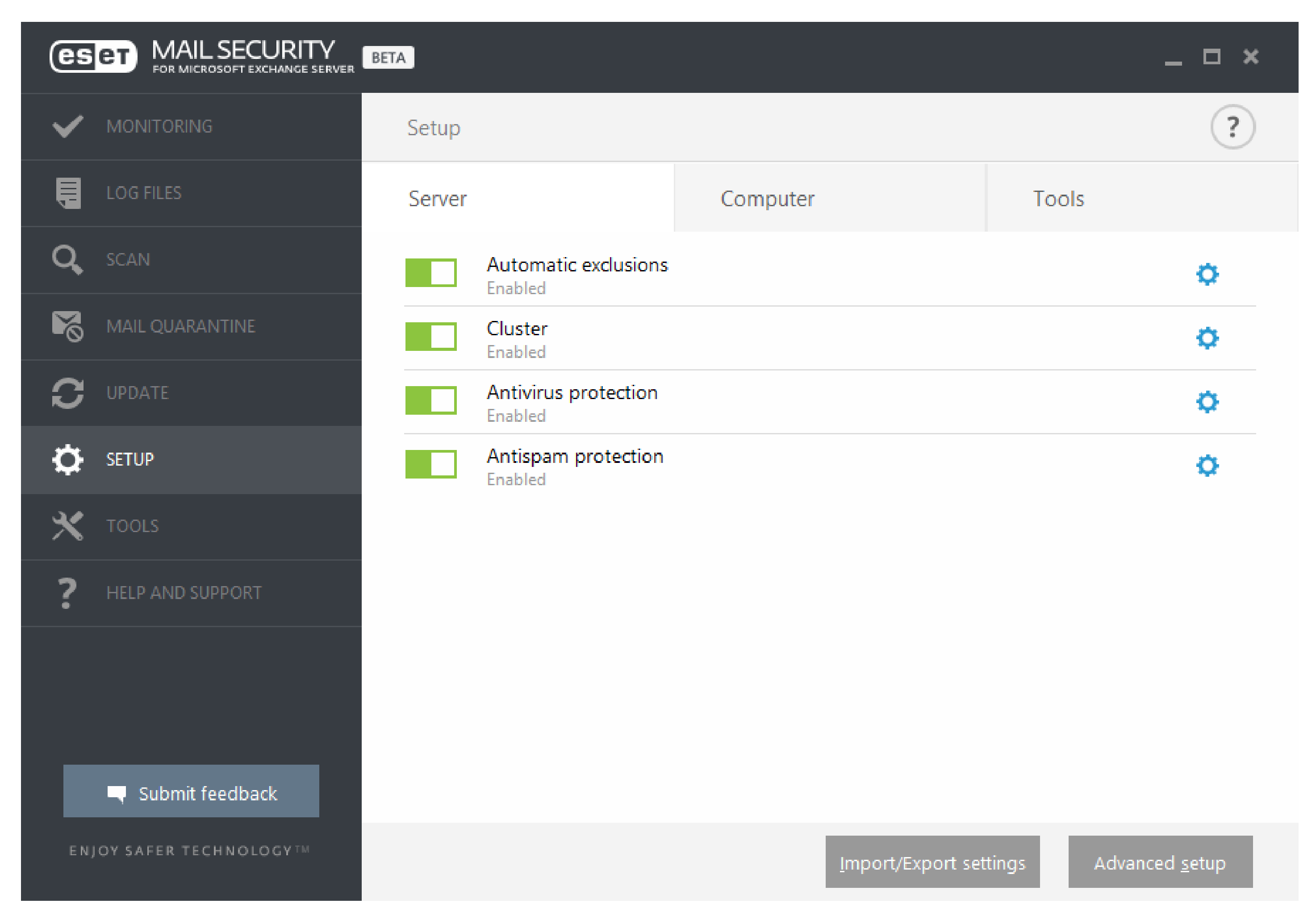


REMARQUE : lorsque vous tentez d'utiliser une installation à distance automatique pour un nœud doté d'une autre plateforme (32 bits par rapport à 64 bits), le programme le détecte et recommande une installation manuelle pour ce nœud.

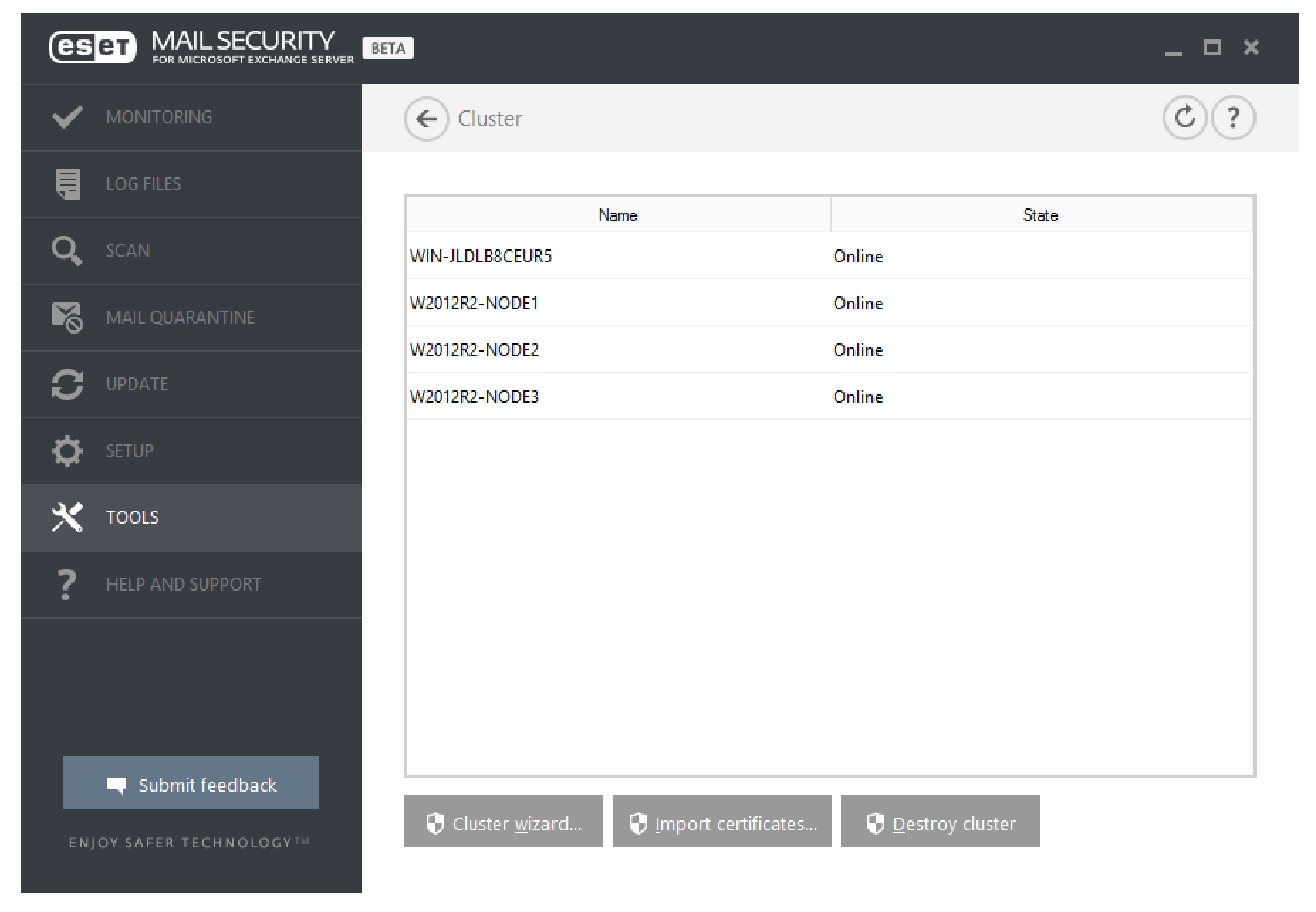
REMARQUE : si une ancienne version de ESET Mail Security est déjà installée sur certains nœuds, une version récente de ESET Mail Security doit être réinstallée sur ces ordinateurs avant de créer le cluster. Cette installation peut entraîner le redémarrage automatique de ces ordinateurs. Si c'est le cas, un avertissement s'affiche.


Cluster - ESET Mail Security
Nodes install and cluster activation
Product install log
[4:53:08 PM] Generating certificates for cluster nodes...
[4:53:11 PM] All certificates created.
[4:53:11 PM] Copying files to remote machines:
[4:53:12 PM] All files have been copied to remote machines.
[4:53:12 PM] Installing product:
[4:53:36 PM] ESET solutions are installed on all remote machines.
[4:53:37 PM] Enrolling certificates:
[4:53:42 PM] All certificates have been enrolled to remote machines.
[4:53:42 PM] Activating cluster feature:
[4:53:48 PM] Cluster feature has been activated on all machines.
[4:53:48 PM] Pushing license to the nodes:
[4:53:49 PM] License has been successfully pushed to the nodes.
[4:53:49 PM] Synchronizing settings:
[4:53:52 PM] Settings have been synchronized.
Install
< Previous
Finish
Cancel

Une fois que vous avez correctement configuré ESET Cluster, il apparaît comme étant activé dans la page **Configuration** > **Serveur**.



Vous pouvez vérifier son état actuel dans la page d'état du cluster (**Outils** > **Cluster**).



Importer les certificats...

- Accédez au dossier contenant les certificats (générés lors de l'utilisation de l'Assistant Cluster).
- Sélectionnez le fichier de certificat, puis cliquez sur **Ouvrir**.

5.2 Ordinateur

Le module **Ordinateur** figure sous **Configuration** > **Ordinateur**. Il donne une vue d'ensemble des modules de protection décrits dans le chapitre précédent. Dans cette section, les paramètres suivants sont disponibles :

- Protection en temps réel du système de fichiers
- Analyse de l’ordinateur à la demande
- Analyse en cas d'inactivité
- Analyse au démarrage
- Supports amovibles
- Protection des documents
- HIPS

Les **options du scanner** pour tous les modules de protection (par exemple, protection en temps réel du système de fichiers, protection de l'accès Web, etc.) vous permettent d'activer ou de désactiver la détection des éléments suivants :

- Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur.
  Pour en savoir plus sur ces types d'applications, consultez le glossaire.
- Les applications potentiellement dangereuses sont des logiciels commerciaux légitimes susceptibles d'être utilisés à des fins malveillantes. Cette catégorie comprend les programmes d'accès à distance, les applications de décodage des mots de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de

l'utilisateur). Cette option est désactivée par défaut.
Pour en savoir plus sur ces types d'applications, consultez le glossaire.

- **Les applications potentiellement suspectes** comprennent des programmes compressés par des compresseurs ou par des programmes de protection. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner leur détection.

La **technologie Anti-Stealth** est un système sophistiqué assurant la détection de programmes dangereux, les rootkits, qui sont à même de se cacher du système d'exploitation, ce qui rend leur détection impossible à l'aide de techniques de test ordinaires.

L'option Exclusions des processus vous permet d'exclure des processus spécifiques. Vous pouvez par exemple exclure les processus de la solution de sauvegarde. Toutes les opérations sur les fichiers de ces processus exclus sont ainsi ignorées et considérées comme étant sûres, ce qui limite l'interférence avec le processus de sauvegarde.

Les exclusions permettent d'exclure des fichiers et dossiers de l'analyse. Pour que la détection des menaces s'applique bien à tous les objets, il est recommandé de ne créer des exclusions que lorsque cela s'avère absolument nécessaire. Certaines situations justifient l'exclusion d'un objet. Par exemple, lorsque les entrées de bases de données volumineuses risquent de ralentir l'ordinateur pendant l'analyse ou lorsqu'il peut y avoir conflit entre le logiciel et l'analyse. Pour obtenir des instructions afin d'exclure un objet de l'analyse, reportez-vous à la section Exclusions.

5.2.1 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Comportement standard

Pour illustrer de manière générale la prise en charge des infiltrations par ESET Mail Security, celles-ci peuvent être détectées à l'aide de :

- Protection en temps réel du système de fichiers
- Protection de l'accès Web
- Protection du client de messagerie
- Analyse de l'ordinateur à la demande

Chaque fonction utilise le niveau de nettoyage standard et tente de nettoyer le fichier et de le déplacer en Quarantaine ou met fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans l'angle inférieur droit de l'écran. Pour plus d'informations sur les niveaux et le comportement de nettoyage, voir Nettoyage.

Nettoyage et suppression

Si aucune action n'est prédéfinie pour le module de protection en temps réel du système de fichiers, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car cette option laissera les fichiers infectés non nettoyés. La seule exception concerne les situations où vous êtes sûr qu'un fichier est inoffensif et qu'il a été détecté par erreur.

Utilisez le nettoyage si un fichier sain a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il est supprimé.

Si un fichier infecté est « verrouillé » ou utilisé par un processus système, il n'est généralement supprimé qu'après avoir été déverrouillé (normalement, après un redémarrage du système).

Menaces multiples

Si des fichiers infectés n'ont pas été nettoyés durant une analyse de l'ordinateur (ou si le niveau de nettoyage a été défini sur **Pas de nettoyage**), une fenêtre d'alerte s'affiche ; elle vous invite à sélectionner des actions pour ces

fichiers. Sélectionnez des actions pour les fichiers (les actions sont définies pour chaque fichier de la liste), puis cliquez sur **Terminer**.

Suppression de fichiers dans les archives

En mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Soyez prudent si vous choisissez un nettoyage strict ; dans ce mode, une archive sera supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

- Ouvrez ESET Mail Security et cliquez sur Analyse de l'ordinateur
- Cliquez sur **Analyse intelligente** (pour plus d'informations, voir Analyse de l'ordinateur)
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

5.2.2 Exclusions des processus

Cette fonctionnalité permet d'exclure des processus d'applications de l'analyse antivirus à l'accès. Ces exclusions réduisent le risque de conflits potentiels et augmentent les performances des applications exclues, ce qui a un effet positif sur les performances globales du système d'exploitation.

Lorsqu'un processus est exclu, le fichier exécutable de ce dernier n'est pas surveillé. L'activité du processus exclu n'est pas surveillée par ESET Mail Security et aucune analyse n'est effectuée sur les opérations sur les fichiers exécutées par le processus.

Utilisez les commandes **Ajouter**, **Modifier** et **Supprimer** pour gérer les exclusions des processus.

REMARQUE : les exclusions des processus sont des exclusions de l'analyse antivirus à l'accès uniquement. Par exemple, la protection de l'accès Web ne prend pas en compte ces exclusions. Par conséquent, si vous excluez le fichier exécutable de votre navigateur Web, les fichiers téléchargés sont toujours analysés. Une infiltration peut ainsi être toujours détectée. Ce scénario est utilisé à titre d'exemple uniquement. Il n'est pas recommandé de créer des exclusions pour les navigateurs Web.

REMARQUE : le système HIPS est impliqué dans l'évaluation des processus exclus. Pour cette raison, il est recommandé de tester les processus nouvellement exclus avec le système HIPS activé (ou désactivé si vous rencontrez des problèmes). La désactivation du système HIPS n'a aucune incidence sur les exclusions de processus. Si le système HIPS est désactivé, l'identification des processus exclus reposent uniquement sur le chemin d'accès.

5.2.3 Exclusions automatiques

Les développeurs d'applications et de systèmes d'exploitation serveur recommandent d'exclure des analyses antivirus les ensembles de dossiers et fichiers de travail critiques pour la plupart de leurs produits. Les analyses antivirus peuvent avoir une influence négative sur les performances d'un serveur, ce qui peut provoquer des conflits et même empêcher l'exécution de certaines applications sur le serveur. Les exclusions permettent de réduire le risque de conflits potentiels et d'augmenter les performances globales du serveur lors de l'exécution du logiciel antivirus.

ESET Mail Security identifie les applications serveur et les fichiers du système d'exploitation serveur critiques, puis les ajoute automatiquement à la liste des exclusions. La section **Exclusions automatiques à générer** répertorie les applications serveur détectées pour lesquelles des exclusions ont été créées. Toutes les exclusions automatiques sont activées par défaut. Vous pouvez désactiver/activer chaque application serveur en cliquant sur le bouton bascule afin d'obtenir le résultat suivant :

1. Si l'exclusion d'une application/d'un système d'exploitation reste activée, les fichiers et dossiers critiques correspondants sont ajoutés à la liste des fichiers exclus de l'analyse (**Configuration avancée** > > **Général** > **Exclusions** > **Modifier**). À chaque redémarrage du serveur, le système vérifie automatiquement les exclusions et restaure celles qui auraient pu être supprimées de la liste. Ce paramètre est recommandé si vous souhaitez vous assurer que les exclusions automatiques conseillées sont toujours appliquées.

2. Si l'exclusion d'une application/d'un système d'exploitation est désactivée, les fichiers et dossiers critiques correspondants restent dans la liste des fichiers exclus de l'analyse (**Configuration avancée** > > **Général** > **Exclusions** > **Modifier**). Toutefois, ils ne sont pas vérifiés et renouvelés automatiquement dans la liste **Exclusions** à chaque redémarrage du serveur (reportez-vous au point 1 ci-dessus). Ce paramètre est recommandé pour les utilisateurs avancés qui souhaitent supprimer ou modifier certaines des exclusions standard. Si vous souhaitez supprimer les exclusions de la liste sans redémarrer le serveur, vous devez les supprimer de la liste manuellement (**Configuration avancée** > > **Général** > **Exclusions** > **Modifier**).

Toutes les exclusions définies par l'utilisateur et saisies manuellement (dans **Configuration avancée** > > **Général** > **Exclusions** > **Modifier**) ne sont pas concernées par les paramètres décrits ci-dessus.

Les exclusions automatiques des applications/systèmes d'exploitation serveur sont sélectionnées en fonction des recommandations de Microsoft. Pour plus d'informations, consultez les articles suivants de la base de connaissances Microsoft :

- Recommandations d'analyse antivirus pour les ordinateurs d'entreprise qui exécutent les versions de Windows prises en charge
- Recommandations pour dépanner un ordinateur Exchange Server avec un logiciel antivirus installé
- Analyse antivirus au niveau fichier sur Exchange 2007
- Logiciel antivirus du système d'exploitation sur les serveurs Exchange

5.2.4 Cache local partagé

Le cache local partagé permet d'accroître considérablement les performances dans les environnements virtualisés en éliminant les analyses en double sur le réseau. Cela permet de s'assurer que chaque fichier est analysé une seule fois et stocké dans le cache partagé. Activez le bouton bascule **Option de mise en cache** pour enregistrer dans le cache local des informations sur les analyses des fichiers et des dossiers sur le réseau. Si vous effectuez une nouvelle analyse, ESET Mail Security recherche les fichiers analysés dans le cache. Si les fichiers correspondent, ils sont exclus de l'analyse.

La **configuration du serveur de cache** comprend les éléments suivants **:**

- **Nom de l'hôte** - Nom ou adresse IP de l'ordinateur sur lequel se trouve le cache.
- **Port** - Numéro de port utilisé pour les communications (identique à celui défini dans le cache local partagé).
- **Mot de passe** - Indiquez le mot de passe du cache local partagé si nécessaire.

5.2.5 Performances

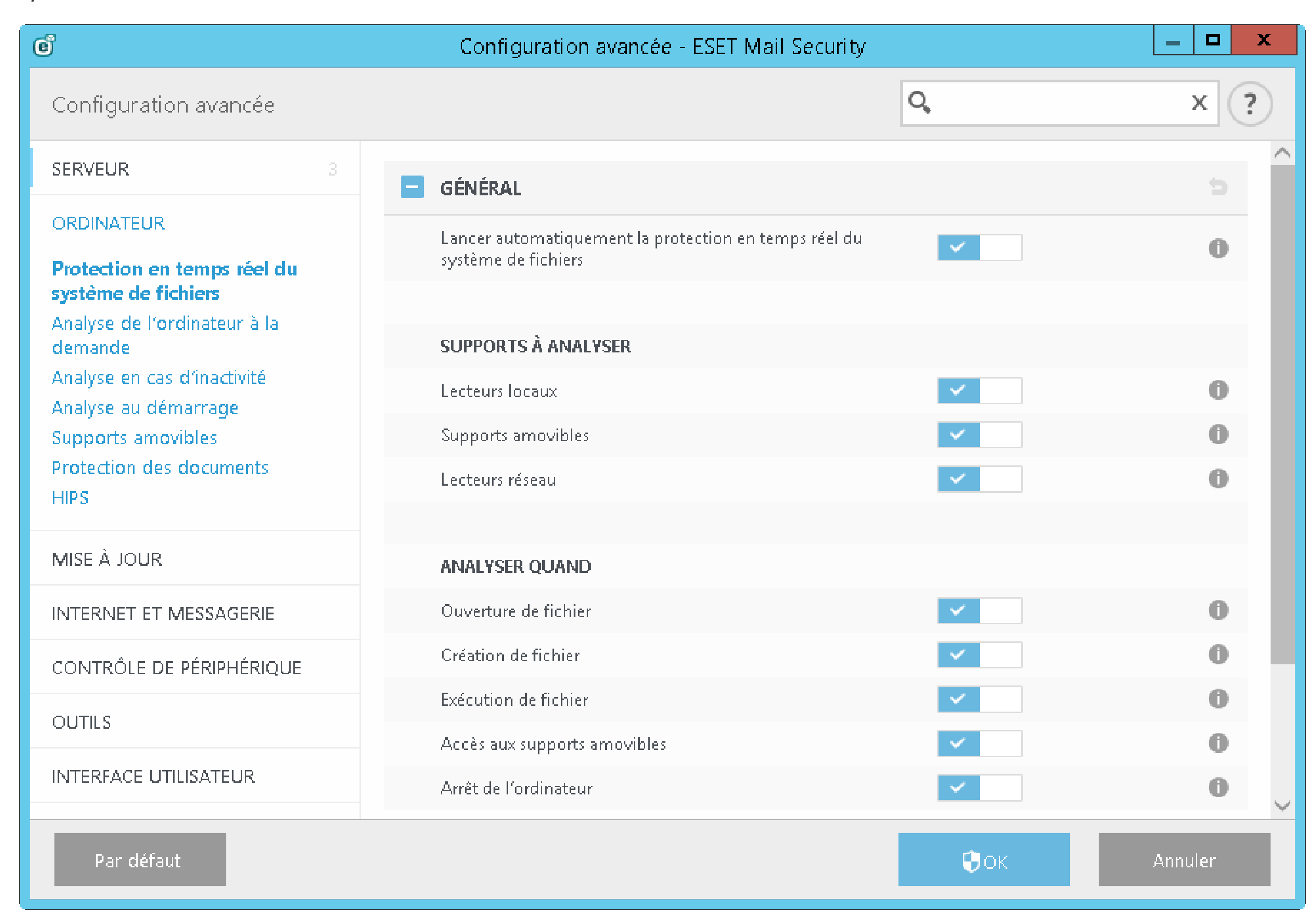
Vous pouvez définir un nombre de moteurs d'analyse ThreatSense indépendants utilisés simultanément par la protection antivirus et antispyware.

S'il n'existe aucune autre restriction, il est recommandé d'augmenter le nombre de moteurs d'analyse ThreatSense selon cette formule : *nombre de moteurs d'analyse ThreatSense = (nombre d'unités centrales physiques x 2) + 1*.

i **REMARQUE** : les valeurs acceptables sont comprises entre 1 et 20. Par conséquent, le nombre maximal de moteurs d'analyse ThreatSense que vous pouvez utiliser est de 20.

5.2.6 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Lorsque ces fichiers sont ouverts, créés ou exécutés sur l'ordinateur, elle les analyse pour y rechercher la présence éventuelle de code malveillant. La protection en temps réel du système de fichiers est lancée au démarrage du système.



Par défaut, la protection en temps réel du système de fichiers est lancée au démarrage du système et assure une analyse ininterrompue. Dans certains cas particuliers (par exemple, en cas de conflit avec un autre scanner en temps réel), la protection en temps réel peut être désactivée en désélectionnant **Démarrer automatiquement la protection en temps réel du système de fichiers** sous **Protection en temps réel du système de fichiers** > **General** dans Configuration avancée.

- **Supports à analyser**

Par défaut, tous les types de supports font l'objet de recherches de menaces potentielles :

Disques locaux - Contrôle tous les disques durs système.
Supports amovibles - Contrôle les CD/DVD, les périphériques USB, les périphériques Bluetooth, etc.
Disques réseau - Analyse tous les lecteurs mappés.

Il est recommandé d'utiliser les paramètres par défaut et de ne les modifier que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

- **Analyser quand**

Par défaut, tous les fichiers sont analysés lors de leur ouverture, création ou exécution. Il est recommandé de conserver ces paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur :

- **Ouverture de fichier** - Active/désactive l'analyse lorsque des fichiers sont ouverts.
- **Création de fichier** - Active/désactive l'analyse lorsque des fichiers sont créés.
- **Exécution de fichier** - Active/désactive l'analyse lorsque des fichiers sont exécutés.
- **Accès aux supports amovibles** - Active/désactive l'analyse déclenchée par l'accès à des supports amovibles spécifiques disposant d'espace de stockage.
- **Arrêt de l'ordinateur** - Active/désactive l'analyse déclenchée par l'arrêt de l'ordinateur.

La protection en temps réel du système de fichiers vérifie tous les types de supports. Elle est déclenchée par différents événements système, tels que l'accès à un fichier. Grâce aux méthodes de détection de la technologie ThreatSense (décrites dans la section Paramètres ThreatSense), la protection du système de fichiers en temps réel peut être configurée pour traiter différemment les nouveaux fichiers et les fichiers existants. Par exemple, vous pouvez configurer la protection en temps réel du système de fichiers pour surveiller plus étroitement les nouveaux fichiers.

Pour garantir un impact minimal de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus. Ce comportement est contrôlé à l'aide de l'**optimisation intelligente**. Si l'optimisation intelligente est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier ce paramètre, appuyez sur **F5** pour ouvrir la configuration avancée, puis développez **Antivirus** > **Protection en temps réel du système de fichiers**. Cliquez ensuite sur **Paramètres ThreatSense** > **Autre**, puis sélectionnez ou désélectionnez **Activer l'optimisation intelligente**.

5.2.6.1 Exclusions

À ne pas confondre avec **Extensions exclues**

Les exclusions permettent d'exclure des fichiers et dossiers de l'analyse. Pour que la détection des menaces s'applique bien à tous les objets, il est recommandé de ne créer des exclusions que lorsque cela s'avère absolument nécessaire. Certaines situations justifient l'exclusion d'un objet. Par exemple, lorsque les entrées de bases de données volumineuses risquent de ralentir l'ordinateur pendant l'analyse ou lorsqu'il peut y avoir conflit entre le logiciel et l'analyse (par exemple, logiciel de sauvegarde).

Pour exclure un objet de l'analyse :

Cliquez sur **Ajouter** et entrez le chemin d'un objet ou sélectionnez-le dans l'arborescence.
Vous pouvez utiliser des caractères génériques pour indiquer un groupe de fichiers. Un point d'interrogation (?) représente un seul caractère variable tandis qu'un astérisque (*) représente une chaîne variable de zéro caractère ou plus.

Exemples

- Si vous souhaitez exclure tous les fichiers d'un dossier, tapez le chemin d'accès au dossier et utilisez le masque « *.* ».
- Pour exclure un disque complet avec tous ses fichiers et sous-dossiers, utilisez le masque « D:\ ».
- Si vous ne souhaitez exclure que les fichiers doc, utilisez le masque « *.doc ».
- Si le nom d'un fichier exécutable comporte un certain nombre de caractères variables dont vous ne connaissez que le premier (par exemple « D »), utilisez le format suivant : « D????.exe ». Les points d'interrogation remplacent les caractères manquants (inconnus).

i **REMARQUE :** une menace présente dans un fichier n'est pas détectée par le module de protection du système de fichiers en temps réel ou par le module d'analyse de l'ordinateur si le fichier en question répond aux critères d'exclusion de l'analyse.

Colonnes

Chemin - Chemin d'accès aux fichiers et dossiers exclus.
Menace - Si le nom d'une menace est affiché en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus. Ce type d'exclusion ne peut être utilisé que pour certains types d'infiltrations. Il peut être créé soit dans la fenêtre des alertes de menaces qui signale l'infiltration (cliquez sur **Afficher les options avancées** et sélectionnez **Exclure de la détection**), soit en cliquant sur **Configuration** > **Quarantaine** à l'aide d'un clic droit sur le fichier placé en quarantaine et en sélectionnant **Restaurer et exclure de la détection** dans le menu contextuel.

Éléments de commande

Ajouter - Exclut les objets de la détection.
Modifier - Permet de modifier des entrées sélectionnées.
Supprimer - Supprime les entrées sélectionnées.

5.2.6.1.1 Ajouter ou modifier une exclusion

Cette boîte de dialogue permet d'ajouter ou de modifier des exclusions. Cette opération peut s'effectuer de deux manières :

- en tapant le chemin d'accès à un objet à exclure ;
- en sélectionnant l'objet dans l'arborescence (cliquez sur l'option **...** à l'extrémité du champ de texte pour accéder à la fonction de navigation).

Si vous utilisez la première méthode, vous pouvez utiliser les caractères génériques décrits dans la section Format d'exclusion.

5.2.6.1.2 Format d'exclusion

Vous pouvez utiliser des caractères génériques pour indiquer un groupe de fichiers. Un point d'interrogation (?) représente un seul caractère variable tandis qu'un astérisque (*) représente une chaîne variable de zéro caractère ou plus.

Exemples

- Si vous souhaitez exclure tous les fichiers d'un dossier, tapez le chemin d'accès au dossier et utilisez le masque « *.* ».
- Pour exclure un disque complet avec tous ses fichiers et sous-dossiers, utilisez le masque « D:\ ».
- Si vous ne souhaitez exclure que les fichiers doc, utilisez le masque « *.doc ».
- Si le nom d'un fichier exécutable comporte un certain nombre de caractères variables dont vous ne connaissez que le premier (par exemple « D »), utilisez le format suivant : « D????.exe ». Les points d'interrogation remplacent les caractères manquants (inconnus).

5.2.6.2 Paramètres ThreatSense

ThreatSense est une technologie constituée de nombreuses méthodes complexes de détection de menaces. C'est une technologie proactive : elle fournit une protection dès le début de la propagation d'une nouvelle menace. Elle utilise une combinaison d'analyse de code, d'émulation de code, de signatures génériques et de signatures de virus qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration du moteur ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- Les types de fichiers et les extensions à analyser
- La combinaison de plusieurs méthodes de détection
- Les niveaux de nettoyage, etc.

Pour ouvrir la fenêtre de configuration, cliquez sur **Configuration des paramètres du moteur ThreatSense** dans la fenêtre de configuration avancée de chaque module utilisant la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Analyse en cas d'inactivité
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l'accès Web
- Analyse de l'ordinateur

Les paramètres ThreatSense sont spécifiquement optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés par un compresseur d'exécutables ou pour autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système (normalement, seuls les fichiers nouvellement créés sont analysés par ces méthodes). Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Objets à analyser

Cette section permet de définir les fichiers et les composants de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.

- **Mémoire vive** - Lance une analyse visant à rechercher les menaces qui attaquent la mémoire vive du système.
- **Secteurs d'amorçage** - Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de virus dans l'enregistrement d'amorçage principal.
- **Fichiers des courriers électroniques** - Le programme prend en charge les extensions suivantes : DBX (Outlook Express) et EML.
- **Archives** - Le programme prend en charge les extensions suivantes : ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE et de nombreuses autres extensions.
- **Archives auto-extractibles** - Les archives auto-extractibles (SFX) n'ont pas besoin de programmes spécialisés pour être décompressées.
- **Fichiers exécutables compressés** - Contrairement aux archiveurs standard, ces fichiers se décompressent en mémoire. Outre les compacteurs statiques standard (UPX, yoda, ASPack, FSG, etc.), l'analyseur peut reconnaître plusieurs autres types de compacteurs via l'utilisation de l'émulation de code.

Options d'analyse

Sélectionnez les méthodes à utiliser lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

- **Heuristique** - La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Elle présente l'avantage d'identifier un code malveillant qui n'existait pas ou qui n'était pas connu par la base de signatures de virus antérieure. Cette méthode présente néanmoins l'inconvénient d'une probabilité (très faible) de fausses alarmes.
- **Heuristique avancée/ADN/Signatures intelligentes** - La méthode heuristique avancée utilise un algorithme heuristique développé par ESET, optimisé pour la détection des vers d'ordinateur et des chevaux de Troie, et écrit dans un langage de programmation de haut niveau. L'utilisation de la méthode heuristique avancée accroît de manière significative les possibilités de détection des menaces des produits ESET. Les signatures peuvent détecter et identifier les virus avec grande efficacité. Grâce au système de mise à jour automatique, les nouvelles signatures peuvent être disponibles dans les quelques heures qui suivent la détection des menaces. L'inconvénient des signatures est qu'elles ne détectent que les virus qu'elles connaissent (ou leurs versions légèrement modifiées).

Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres (contextuelles, publicitaires) ;
- activation et exécution de processus cachés ;
- augmentation de l'utilisation des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

- **Applications potentiellement dangereuses** - La classification Applications potentiellement dangereuses est utilisée pour les logiciels commerciaux légitimes, tels que les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers ((programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Cette option est désactivée par défaut.
- **ESET Live Grid** - Grâce à la technologie de réputation d'ESET, les informations sur les fichiers analysés sont comparées aux données issues du système ESET Live Grid basé sur le cloud computing. Cette comparaison permet d'améliorer la détection tout en accélérant l'analyse.

Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :

Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

Nettoyage normal - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d'une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par une notification affichée dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une action prédéfinie ne peut pas être menée à bien.

Nettoyage strict - Le programme nettoie ou supprime tous les fichiers infectés. Les seules exceptions sont les fichiers système. Si un fichier ne peut pas être nettoyé, l'application demande à l'utilisateur le type d'opération à effectuer.

Avertissement : si une archive contient un ou plusieurs fichiers infectés, elle peut être traitée de deux façons. En mode standard (Nettoyage standard), toute l'archive est supprimée si tous ses fichiers sont infectés. En mode de **nettoyage strict**, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers contenus.

Exclusions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

Lorsque vous configurez les paramètres du moteur ThreatSense pour l'analyse à la demande d'un ordinateur, vous disposez également des options de la section **Autre** suivantes :

- **Analyser les flux de données alternatifs (ADS)** - Les flux de données alternatifs (ADS) utilisés par le système de fichiers NTFS sont des associations de fichiers et de dossiers que les techniques d'analyse ordinaires ne permettent pas de détecter. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.
- **Exécuter les analyses en arrière-plan avec une priorité faible** - Toute séquence d'analyse consomme une certaine quantité de ressources système. Si vous utilisez des programmes qui exigent une grande quantité de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.
- **Journaliser tous les objets** - Si cette option est sélectionnée, le fichier journal affiche tous les fichiers analysés, même ceux qui ne sont pas infectés. Par exemple, si une infiltration est détectée dans une archive, le journal répertorie également les fichiers nettoyés contenus dans l'archive.
- **Activer l'optimisation intelligente** - Lorsque cette option est sélectionnée, les paramètres optimaux sont utilisés de manière à garantir le niveau d'analyse le plus efficace tout en conservant la meilleure vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes et en les appliquant à des types de fichiers spécifiques. Si l'option Activer l'optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau ThreatSense des différents modules sont appliqués lors de la réalisation d'une analyse.
- **Conserver la date et l'heure du dernier accès** - Sélectionnez cette option pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de les mise à jour (par exemple, pour les utiliser avec des systèmes de sauvegarde de données).

Limites

La section Limites permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

Paramètres d'objet

Paramètres d'objet par défaut

- **Taille maximale d'objet** - Définit la taille maximale des objets à analyser. Le module antivirus n'analyse que les objets d'une taille inférieure à celle spécifiée. Cette option ne doit être modifiée que par des utilisateurs expérimentés et qui ont des raisons particulières d'exclure de l'analyse des objets de plus grande taille. Valeur par défaut : *illimité*.
- **Durée d'analyse maximale pour l'objet (s)** - Définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non. Valeur par défaut : *illimité*.

Configuration de l'analyse d'archive

Niveau d'imbrication des archives - Spécifie la profondeur maximale d'analyse des archives. Valeur par défaut : *10*.

Taille maximale de fichier dans l'archive - Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. Valeur par défaut : *illimité*.

REMARQUE : il n'est pas recommandé de modifier les valeurs par défaut. Dans des circonstances normales, il n'y a aucune raison de le faire.

5.2.6.2.1 Extensions exclues

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.

Par défaut, tous les fichiers sont analysés. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse.

L'exclusion de fichiers peut être utile si l'analyse de certains types de fichiers provoque un dysfonctionnement de l'application utilisant certaines extensions. Par exemple, il peut être judicieux d'exclure les extensions .edb, .eml et .tmp si vous utilisez des serveurs Microsoft Exchange.

Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des fichiers portant certaines extensions. Pour ajouter une nouvelle extension à la liste, cliquez sur Ajouter, tapez l'extension dans le champ correspondant, puis cliquez sur OK. Lorsque vous sélectionnez **Entrer plusieurs valeurs**, vous pouvez ajouter plusieurs extensions de fichier en les séparant par des lignes, des virgules ou des points-virgules. Lorsque la sélection multiple est activée, les extensions s'affichent dans la liste. Sélectionnez une extension dans la liste, puis cliquez sur **Supprimer** pour la supprimer de la liste. Si vous souhaitez modifier une extension sélectionnée, cliquez sur **Modifier**.

Vous ne pouvez pas utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque représente n'importe quelle chaîne de caractères, tandis que le point d'interrogation symbolise n'importe quel caractère.

5.2.6.2.2 Autres paramètres ThreatSense

Autres paramètres ThreatSense pour les fichiers nouveaux et les fichiers modifiés - La probabilité d'infection des nouveaux fichiers ou des fichiers modifiés est comparativement plus élevée que dans les fichiers existants. C'est la raison pour laquelle le programme vérifie ces fichiers avec des paramètres d'analyse supplémentaires. Outre les méthodes d'analyse basées sur les signatures, le système utilise également l'heuristique avancée qui permet de détecter les nouvelles menaces avant la mise à disposition de la mise à jour de la base des signatures de virus. Outre les nouveaux fichiers, l'analyse porte également sur les fichiers auto-extractibles (.sfx) et les fichiers exécutables compressés (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Pour modifier les paramètres d'analyse d'archive, désactivez **Paramètres d'analyse d'archive par défaut**.

Pour plus d'informations sur les **fichiers exécutables compressés**, les **archives auto-extractibles** et l'**heuristique avancée**, reportez-vous à la section Configuration des paramètres du moteur ThreatSense.

Autres paramètres ThreatSense pour les fichiers exécutés : par défaut, l'heuristique avancée n'est pas utilisée lors de l'exécution des fichiers. Lorsque ce paramètre est activé, il est fortement recommandé de conserver les options Optimisation intelligente et ESET Live Grid activées pour limiter l'impact sur les performances système.

5.2.6.2.3 Niveaux de nettoyage

La protection en temps réel comporte trois niveaux de nettoyage (pour accéder aux paramètres, cliquez sur **Paramètres ThreatSense** dans la section **Protection en temps réel du système de fichiers**, puis cliquez sur **Nettoyage**).

Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

Nettoyage normal - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d'une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par une notification affichée dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une action prédéfinie ne peut pas être menée à bien.

Nettoyage strict - Le programme nettoie ou supprime tous les fichiers infectés. Les seules exceptions sont les fichiers système. Si un fichier ne peut pas être nettoyé, l'application demande à l'utilisateur le type d'opération à

effectuer.

Avertissement : si une archive contient un ou plusieurs fichiers infectés, elle peut être traitée de deux façons. En mode standard (Nettoyage standard), toute l'archive est supprimée si tous ses fichiers sont infectés. En mode de **nettoyage strict**, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers contenus.

5.2.6.2.4 Quand faut-il modifier la configuration de la protection en temps réel

La protection du système de fichiers en temps réel est le composant essentiel de la sécurisation du système. Procédez toujours avec prudence lors de la modification des paramètres de ce module. Il est recommandé de ne modifier les paramètres que dans des cas très précis.

Après l'installation d'ESET Mail Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur en regard de chaque onglet de la fenêtre (**Configuration avancée** > > **Protection en temps réel du système de fichiers**).

5.2.6.2.5 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et détecte les virus, utilisez un fichier de test d'eicar.com. Ce fichier de test est un fichier inoffensif détectable par tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) et permet de tester la fonctionnalité des programmes antivirus. Le fichier est téléchargeable à partir de la page http://www.eicar.org/download/eicar.com

5.2.6.2.6 Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée

Si la protection en temps réel a été désactivée par mégarde par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** dans la fenêtre principale du programme et cliquez sur **Protection en temps réel du système de fichiers**.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement parce que **Lancer automatiquement la protection en temps réel du système de fichiers** est désactivé. Pour activer cette option, accédez à Configuration avancée (**F5**), puis cliquez sur **Ordinateur** > **Protection en temps réel du système de fichiers** > **General** dans la section **Configuration avancée**. Vérifiez que le bouton bascule **Lancer automatiquement la protection en temps réel du système de fichiers** est activé.

Si la protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système avant d'installer ESET.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si **Lancer automatiquement la protection en temps réel du système de fichiers** est activé), le problème peut provenir de conflits avec d'autres programmes. Afin d'obtenir une assistance pour résoudre ce problème, veuillez contacter le service client d'ESET.

5.2.6.2.7 Soumission

Vous pouvez sélectionner le mode d'envoi des fichiers et des informations statistiques à ESET. Sélectionnez l'option **Via la Console d'administration à distance (RA) ou directement à ESET** pour que les fichiers et les statistiques soient envoyés par tout moyen disponible. Sélectionnez l'option **Via la Console d'administration à distance (RA)** pour envoyer les fichiers et les statistiques au serveur d'administration à distance qui les envoie ensuite au laboratoire de recherche sur les menaces d'ESET. Si l'option **Directement à ESET** est sélectionnée, tous les fichiers suspects et les informations statistiques seront livrés directement par le programme au laboratoire d'ESET.

Si des fichiers sont en attente de soumission, le bouton **Soumettre maintenant** est activé. Cliquez sur ce bouton pour soumettre immédiatement les fichiers et les informations statistiques.

Activez l'option **Activer la journalisation** pour créer un journal permettant d'enregistrer les soumissions des fichiers et des informations statistiques.

5.2.6.2.8 Statistiques

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations anonymes concernant les nouvelles menaces détectées. Ces informations peuvent inclure le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont généralement fournies aux serveurs d'ESET une ou deux fois par jour.

Voici un exemple d'informations statistiques envoyées :

```
# utc_time=2005-04-14 07:21:28
# country="Slovaquie"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Quand soumettre : vous pouvez définir le moment de l'envoi des informations statistiques. Si vous choisissez d'envoyer les informations statistiques **Dès que possible**, elles sont envoyées immédiatement après leur création. Ce choix convient si une connexion Internet est disponible en permanence. Si l'option **Pendant la mise à jour** est sélectionnée, toutes les informations statistiques sont envoyées collectivement pendant la mise à jour suivante.

5.2.6.2.9 Fichiers suspects

L'onglet **Fichiers suspects** permet de configurer la manière dont les menaces sont soumises pour analyse au laboratoire de recherche sur les menaces d'ESET.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. S'il s'agit d'une application malveillante, sa détection est ajoutée à la prochaine mise à jour de la base des signatures de virus.

La soumission des fichiers peut être définie pour se produire automatiquement. Vous pouvez également sélectionner l'option **Demander avant de soumettre** si vous souhaitez connaître les fichiers qui sont envoyés pour analyse et confirmer l'envoi.

Si vous ne souhaitez pas soumettre de fichiers, sélectionnez l'option **Ne pas soumettre pour analyse**. Le fait de choisir de ne pas soumettre les fichiers pour analyse n'a pas d'incidence sur la soumission des informations statistiques qui est configurée indépendamment (reportez-vous à la section Statistiques).

Quand soumettre - par défaut, l'option **Dès que possible** est sélectionnée pour que les fichiers suspects soient envoyés au laboratoire de recherche sur les menaces d'ESET. Ceci est recommandé lorsqu'une connexion Internet permanente est disponible et que les fichiers suspects peuvent être livrés très rapidement. Sélectionnez l'option **Pendant la mise à jour** pour que les fichiers suspects soient téléchargés vers ThreatSense.Net pendant la mise à jour suivante.

Filtre d'exclusion - Cette option permet d'exclure certains fichiers/dossiers de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Adresse de contact - Votre **adresse de contact [facultative]** peut être envoyée avec les fichiers suspects et peut être utilisée pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

5.2.7 Analyse de l'ordinateur à la demande

Les options de cette section permettent de sélectionner des paramètres d'analyse.

Profil sélectionné - Ensemble des paramètres utilisés par l'analyseur à la demande. Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**.

Si vous souhaitez uniquement analyser une cible spécifique, vous pouvez cliquer sur **Modifier** en regard de **Cibles à analyser**, puis sélectionner une option dans le menu déroulant ou choisir des cibles spécifiques dans la structure (arborescence) des dossiers.

La fenêtre des cibles à analyser permet de définir les objets (mémoire, lecteurs, secteurs, fichiers et dossiers) dans lesquels rechercher des infiltrations. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur. Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

- **Par les paramètres de profil** - Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** - Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** - Permet de sélectionner tous les disques durs du système.
- **Disques réseau** - Analyse tous les lecteurs réseau mappés.
- **Dossiers partagés** - Sélectionne tous les dossiers partagés sur le serveur local.
- **Aucune sélection** - Annule toutes les sélections.

Cliquez sur Paramètres ThreatSense pour modifier les paramètres d'analyse (par exemple, les méthodes de détection) pour l'analyse de l'ordinateur à la demande.

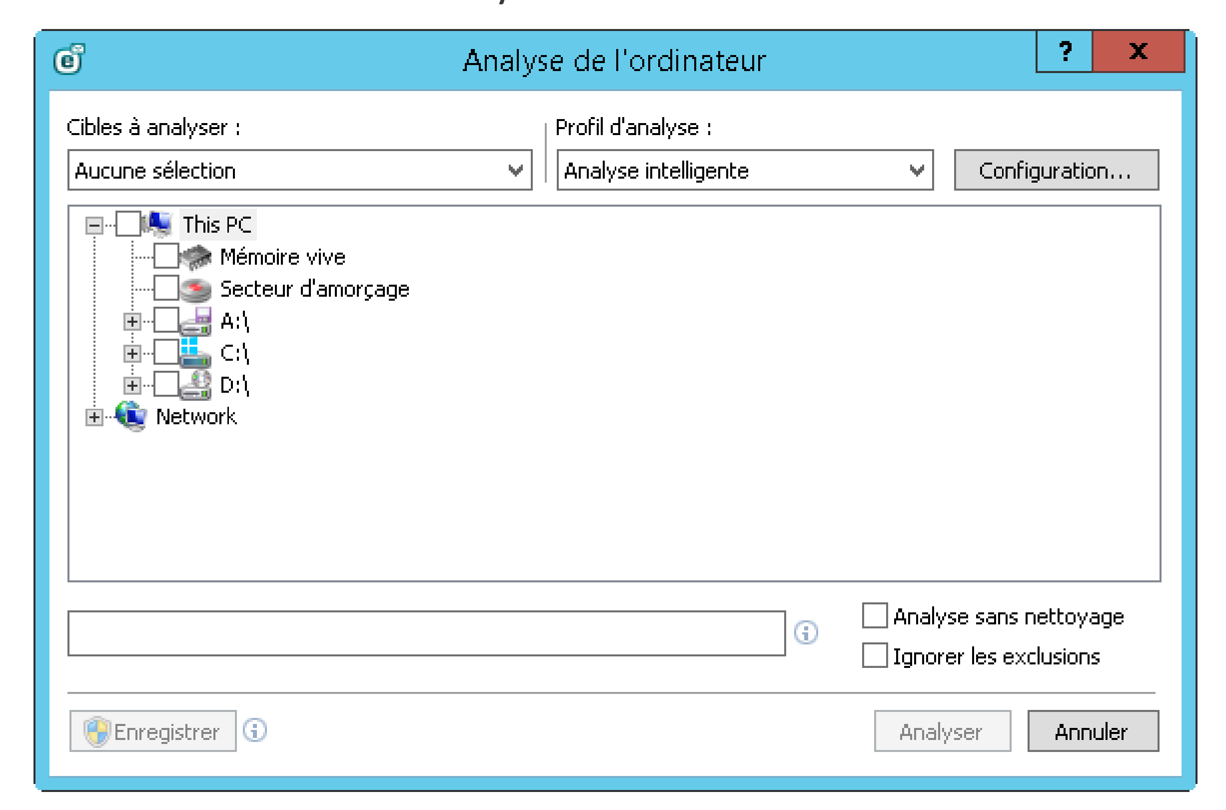
5.2.7.1 Lanceur d'analyses personnalisées

Si vous souhaitez analyser uniquement une cible spécifique, vous pouvez utiliser l'analyse personnalisée en cliquant sur **Analyse d'ordinateur** > **Analyse personnalisée** et sélectionner une option dans le menu déroulant **Cibles à analyser** ou des cibles particulières dans l'arborescence des dossiers.

La fenêtre des cibles à analyser permet de définir les objets (mémoire, lecteurs, secteurs, fichiers et dossiers) dans lesquels rechercher des infiltrations. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur. Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

- **Par les paramètres de profil** - Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** - Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** - Permet de sélectionner tous les disques durs du système.
- **Disques réseau** - Analyse tous les lecteurs réseau mappés.
- **Dossiers partagés** - Sélectionne tous les dossiers partagés sur le serveur local.
- **Aucune sélection** - Annule toutes les sélections.

Pour accéder rapidement à une cible d'analyse ou ajouter directement une cible souhaitée (dossiers ou fichiers), entrez-la dans le champ vide sous la liste de dossiers. Aucune cible ne doit être sélectionnée dans la structure arborescente et le menu **Cibles à analyser** doit être défini sur **Aucune sélection**.



Les fichiers infectés ne sont pas nettoyés automatiquement. Une analyse sans nettoyage permet d'obtenir un aperçu de l'état actuel de la protection. Si vous souhaitez effectuer uniquement une analyse du système sans actions de nettoyage supplémentaires, sélectionnez **Analyse sans nettoyage**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration** > **Paramètres ThreatSense** > **Nettoyage**. Les informations de l'analyse sont enregistrées dans un journal d'analyse.

Vous pouvez choisir un profil à utiliser pour l'analyse des cibles sélectionnées dans le menu déroulant **Profil d'analyse**. Le profil par défaut est **Analyse intelligente**. Il existe deux autres profils d'analyse prédéfinis nommés **Analyse approfondie** et **Analyse via le menu contextuel**. Ces profils d'analyse utilisent différents ThreatSenseparamètres de moteur. Cliquez sur **Configuration...** pour configurer en détail le profil d'analyse de votre choix dans le menu Profil d'analyse. Les options disponibles sont décrites dans la section **Autre** de Configuration des paramètres du moteur ThreatSense.

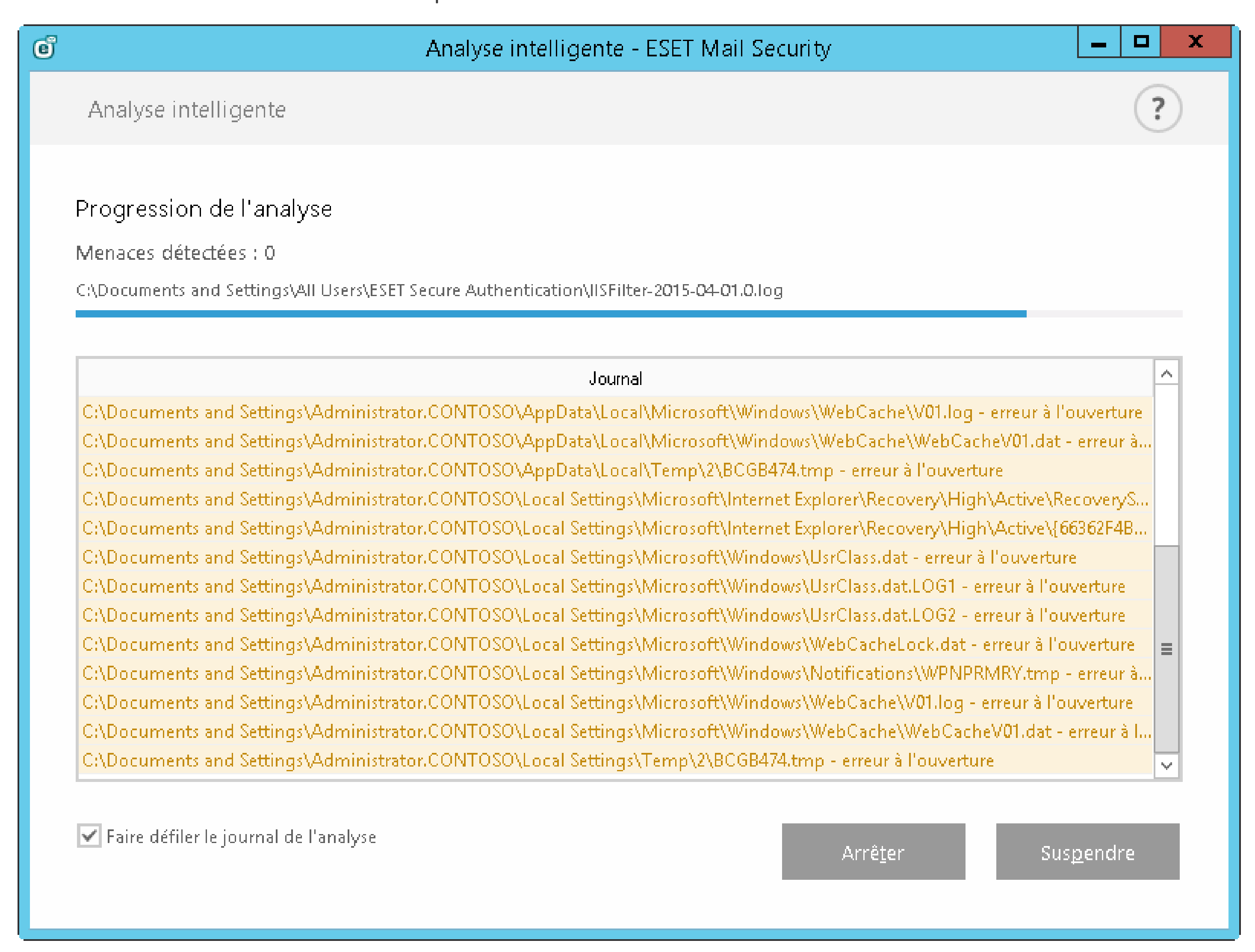
Cliquez sur **Enregistrer** pour enregistrer les modifications apportées à la sélection des cibles, y compris les sélections effectuées dans l'arborescence des dossiers.

Cliquez sur **Analyser** pour exécuter l'analyse avec les paramètres personnalisés que vous avez définis.

Analyser en tant qu'administrateur vous permet d'exécuter l'analyse sous le compte administrateur. Cliquez sur cette option si l'utilisateur actuel ne dispose pas des privilèges suffisants pour accéder aux fichiers à analyser. Remarquez que ce bouton n'est pas disponible si l'utilisateur actuel ne peut pas appeler d'opérations UAC en tant qu'administrateur.

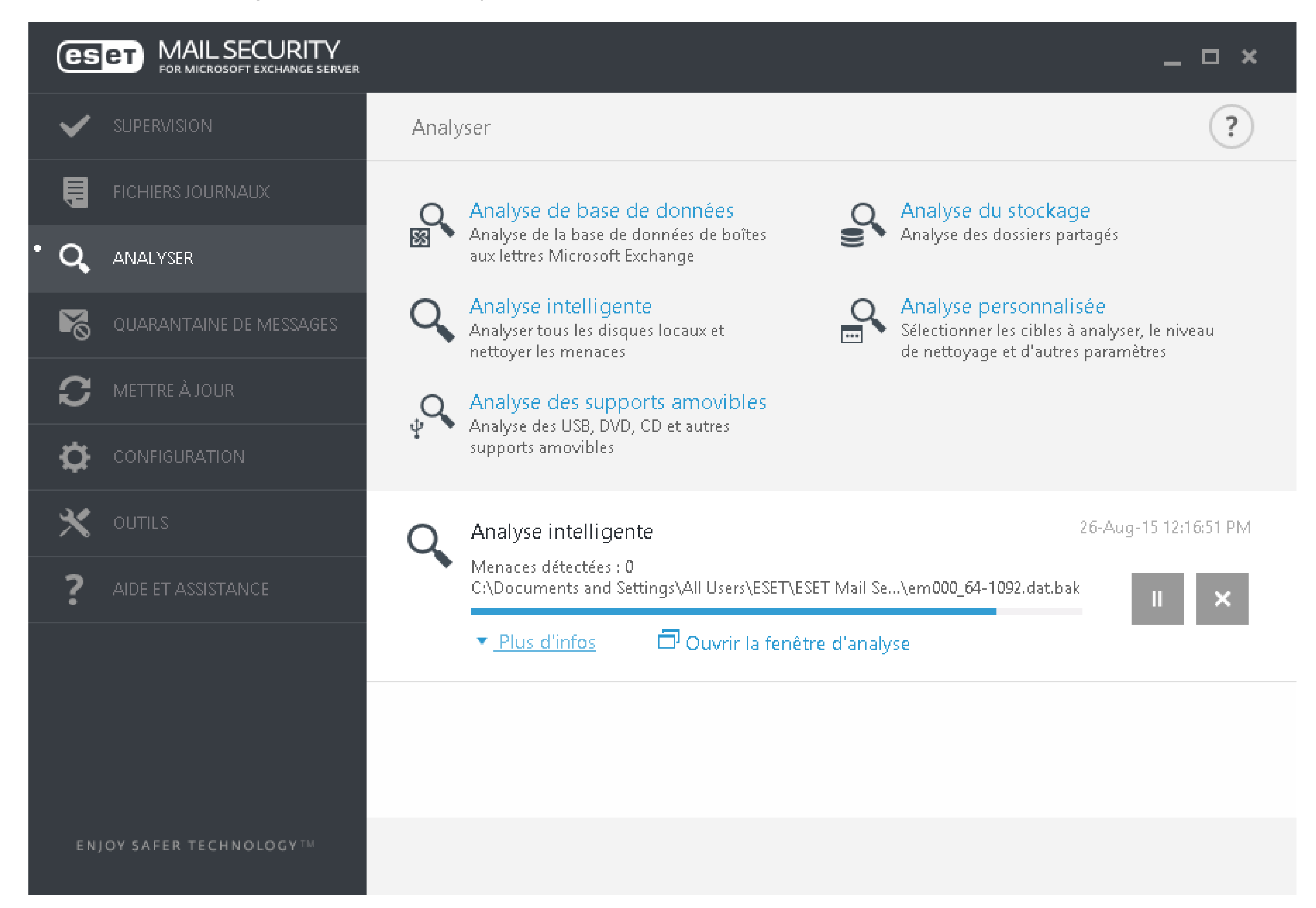
5.2.7.2 Progression de l'analyse

La fenêtre de progression de l'analyse indique l'état actuel de l'analyse, ainsi que des informations sur le nombre de fichiers contenant du code malveillant qui sont détectés.



REMARQUE : il est normal que certains fichiers, protégés par mot de passe ou exclusivement utilisés par le système (en général *pagefile.sys* et certains fichiers journaux), ne puissent pas être analysés.

Progression de l'analyse - La barre de progression indique l'état des objets déjà analysés par rapport aux objets qui ne sont pas encore analysés. L'état de progression de l'analyse est dérivé du nombre total d'objets intégrés dans l'analyse.
Cible - Taille de l'élément analysé et emplacement.
Menaces détectées - Indique le nombre total de menaces détectées pendant une analyse.
Interrompre - Interrompt une analyse.
Reprendre - Cette option est visible lorsque l'analyse est interrompue. Cliquez sur Reprendre pour poursuivre l'analyse.
Arrêter - Met fin à l'analyse.
Faire défiler le journal de l'analyse - Si cette option est activée, le journal de l'analyse défile automatiquement au fur et à mesure de l'ajout des entrées les plus récentes.



5.2.7.3 Gestionnaire de profils

Le gestionnaire de profil est utilisé à deux endroits dans ESET Mail Security - dans les sections **Analyse de l'ordinateur à la demande** et **Mise à jour**.

Analyse de l'ordinateur à la demande

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un nouveau profil, ouvrez la fenêtre Configuration avancée (F5), cliquez sur > **Analyse de l'ordinateur à la demande**, puis sur **Modifier** en regard de **Liste de profils**. Le menu déroulant **Profil sélectionné** répertorie les profils d'analyse existants. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section ThreatSenseConfiguration du moteur ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration

d'analyse intelligente est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **nettoyage strict**. Entrez le nom du nouveau profil dans la fenêtre **Gestionnaire de profils**, puis cliquez sur **Ajouter**. Sélectionnez le nouveau profil dans le menu déroulant **Profil sélectionné** et réglez les paramètres restants selon vos besoin. Cliquez sur **OK** pour enregistrer le nouveau profil.

Mise à jour

L'éditeur de profils de la section de configuration des mises à jour permet aux utilisateurs de créer de nouveaux profils de mise à jour. Il est conseillé de créer et d'utiliser des profils personnalisés (autre que l'option par défaut **Mon profil**) si votre ordinateur utilise plusieurs voies de connexion aux serveurs de mise à jour.

C'est le cas par exemple d'un ordinateur portable qui se connecte normalement à un serveur local (miroir) sur le réseau local, mais qui télécharge les mises à jour directement à partir des serveurs de mise à jour d'ESET lorsqu'il est déconnecté du réseau local (voyage d'affaires). le premier se connectant au serveur local, le second aux serveurs d'ESET. Une fois ces profils configurés, allez dans **Outils** > **Planificateur** puis modifiez les paramètres de mise à jour de la tâche. Désignez un profil comme principal et l'autre comme secondaire.

Profil sélectionné - Le profil de mise à jour utilisé actuellement. Pour le changer, choisissez un profil dans le menu déroulant.

Liste des profils - Permet de créer des profils de mise à jour ou de les modifier.

5.2.7.4 Cibles à analyser

La fenêtre des cibles à analyser permet de définir les objets (mémoire, lecteurs, secteurs, fichiers et dossiers) dans lesquels rechercher des infiltrations. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur. Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

- **Par les paramètres de profil** - Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** - Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** - Permet de sélectionner tous les disques durs du système.
- **Disques réseau** - Analyse tous les lecteurs réseau mappés.
- **Dossiers partagés** - Sélectionne tous les dossiers partagés sur le serveur local.
- **Aucune sélection** - Annule toutes les sélections.

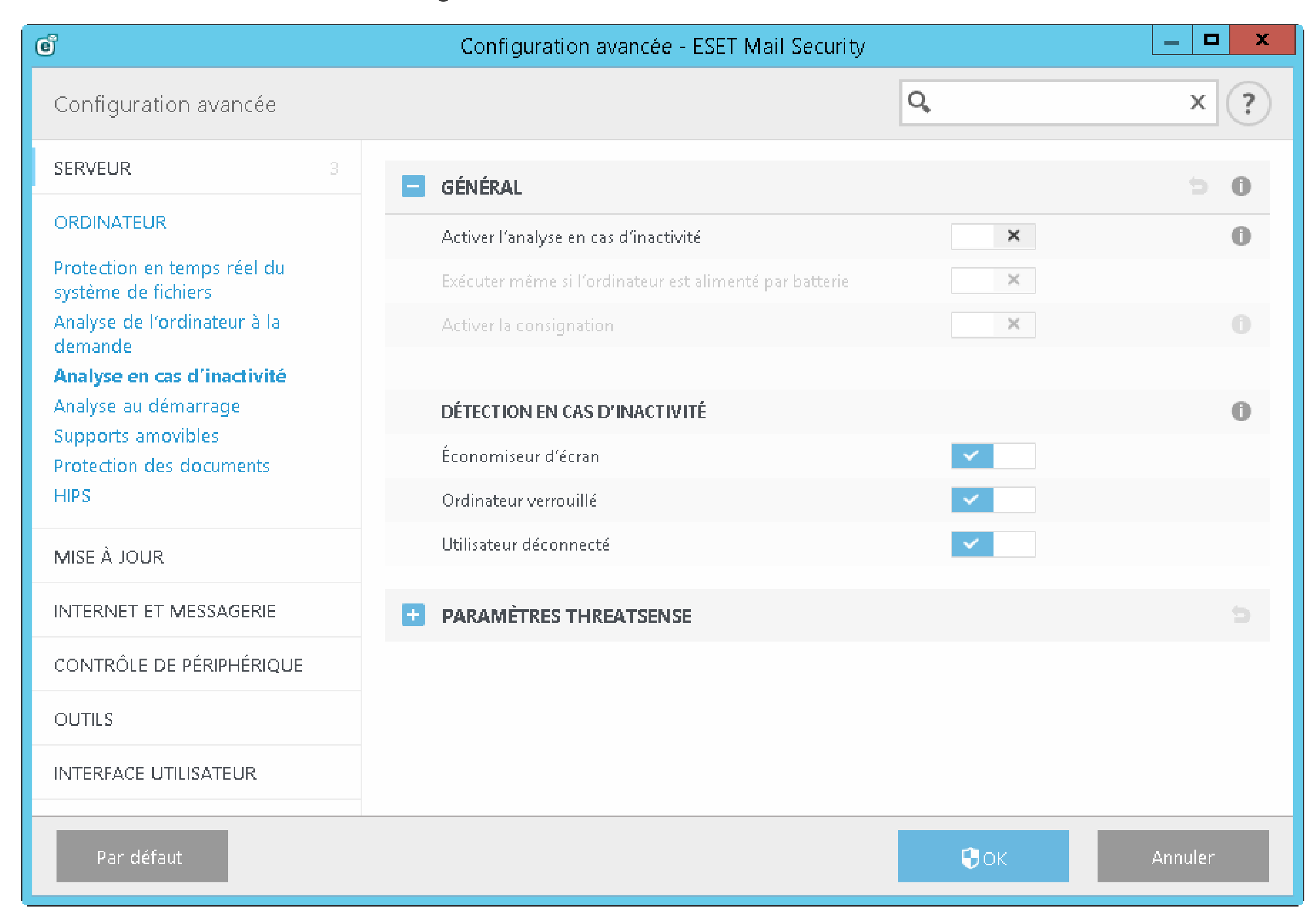
5.2.7.5 Suspendre une analyse planifiée

Une analyse planifiée peut être différée. Indiquez une valeur pour l'option **Arrêter les analyses planifiées dans (min)**, si vous souhaitez différer l'analyse de l'ordinateur.

5.2.8 Analyse en cas d'inactivité

Vous pouvez activer l'analyse en cas d'inactivité dans **Configuration avancée** sous > **Analyse en cas d'inactivité** > **Général**. Placez le bouton bascule en regard de l'option **Activer l'analyse en cas d'inactivité** sur Activer pour activer cette fonctionnalité. Lorsque l'ordinateur n'est pas utilisé, une analyse silencieuse de l'ordinateur est effectuée sur tous les disques locaux.

Par défaut, l'analyse d'inactivité n'est pas exécutée lorsque l'ordinateur (portable) fonctionne sur batterie. Vous pouvez passer outre ce paramètre en activant la case à cocher en regard de l'option **Exécuter même si l'ordinateur est alimenté sur batterie** dans la configuration avancée.



Activez le bouton bascule **Activer la journalisation** dans la configuration avancée pour enregistrer les sorties d'analyse d'ordinateur dans la section Fichiers journaux (dans la fenêtre principale du programme, cliquez sur **Outils** > **Fichiers journaux** et, dans le menu déroulant **Journaliser**, sélectionnez **Analyse de l'ordinateur**).

La détection en cas d'inactivité s'exécute lorsque votre ordinateur se trouve dans l'un des états suivants :

- Économiseur d'écran
- Ordinateur verrouillé
- Utilisateur déconnecté

Cliquez sur Paramètres ThreatSense pour modifier les paramètres d'analyse (par exemple, les méthodes de détection) pour l'analyse en cas d'inactivité.

5.2.9 Analyse au démarrage

Par défaut, la vérification automatique des fichiers au démarrage est effectuée au démarrage du système et lors des mises à jour de la base des signatures de virus. Cette analyse dépend de la configuration et des tâches du Planificateur.

Les options d'analyse au démarrage font partie de la tâche planifiée **Contrôle des fichiers de démarrage du système**. Pour modifier les paramètres d'analyse au démarrage, accédez à **Outils** > **Planificateur**, cliquez sur **Vérification automatique des fichiers de démarrage**, puis sur **Modifier**. À la dernière étape, la fenêtre Vérification des fichiers de démarrage s'affichera (reportez-vous à la section suivante pour plus de détails).

Pour des instructions détaillées sur la création et à la gestion de tâches planifiées, voir Création de nouvelles tâches.

5.2.9.1 Vérification automatique des fichiers de démarrage

Lorsque vous créez une tâche planifiée de contrôle des fichiers au démarrage du système, plusieurs options s'offrent à vous pour définir les paramètres suivants :

Le menu déroulant **Niveau d'analyse** indique le niveau d'analyse appliqué aux fichiers exécutés au démarrage du système. Les fichiers sont organisés par ordre croissant suivant ces critères :

- **Seulement les fichiers utilisés fréquemment** (nombre minimum de fichiers analysés)
- **Fichiers fréquemment utilisés**
- **Fichiers couramment utilisés**
- **Fichiers rarement utilisés**
- **Tous les fichiers enregistrés** (la plupart des fichiers sont analysés)

Il existe en outre deux groupes de **Niveau d'analyse** :

- **Fichiers exécutés avant la connexion de l'utilisateur** - Contient des fichiers situés à des emplacements accessibles sans qu'une session ait été ouverte par l'utilisateur (englobe pratiquement tous les emplacements de démarrage tels que services, objets Application d'assistance du navigateur, notification Winlogon, entrées de planificateur Windows, DLL connues, etc.).
- **Fichiers exécutés après la connexion de l'utilisateur** - Contient des fichiers situés à des emplacements accessibles uniquement après l'ouverture d'une session par l'utilisateur (englobe des fichiers qui ne sont exécutés que pour un utilisateur spécifique, généralement les fichiers de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Les listes des fichiers à analyser sont fixes pour chaque groupe précité.

Priorité d'analyse - Niveau de priorité servant à déterminer le démarrage d'une analyse :

- **Normale** - lorsque le système est moyennement chargé,
- **Faible** - lorsque le système est faiblement chargé,
- **La plus faible** - lorsque la charge du système est la plus faible possible,
- **En période d'inactivité** - la tâche n'est accomplie que lorsque le système n'est pas utilisé.

5.2.10 Supports amovibles

ESET Mail Security permet d'analyser automatiquement les supports amovibles (CD/DVD/USB). Ce module permet d'analyser un support inséré. Cela peut être utile si l'administrateur souhaite empêcher les utilisateurs d'utiliser des supports amovibles avec du contenu non sollicité.

Action à entreprendre après l'insertion de support amovible - Sélectionnez l'action par défaut qui sera exécutée lors de l'insertion d'un support amovible (CD/DVD/USB). Si l'option **Afficher les options d'analyse** est sélectionnée, une notification vous autorise à choisir l'action adéquate :

- **Ne pas analyser** - Aucune action n'est exécutée et la fenêtre **Nouveau périphérique détecté** se ferme.
- **Analyse automatique de périphérique** - Le support amovible inséré fait l'objet d'une analyse à la demande.
- **Afficher les options d'analyse** - Ouvre la section de configuration des supports amovibles.

Lorsqu'un support amovible est inséré, la boîte de dialogue suivante s'affiche :

- **Analyser maintenant** - Cette option déclenche l'analyse du support amovible.
- **Analyser ultérieurement** - L'analyse du support amovible est reportée.
- **Configuration** - Ouvre la boîte de dialogue Configuration avancée.
- **Toujours utiliser l'option sélectionnée** - Lorsque cette option est sélectionnée, la même action sera exécutée lorsqu'un support amovible sera inséré plus tard.

En outre, ESET Mail Security offre la fonctionnalité de contrôle des périphériques qui permet de définir des règles d'utilisation de périphériques externes sur un ordinateur donné. Pour plus de détails sur le contrôle des périphériques, reportez-vous à la section Contrôle des périphériques.

5.2.11 Protection des documents

La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que des éléments Microsoft ActiveX. La protection des documents fournit une couche de protection supplémentaire qui vient s'ajouter à la protection en temps réel du système de fichiers. Elle peut être désactivée pour améliorer la performance des systèmes qui ne sont pas exposés à un grand nombre de documents Microsoft Office.

- **Intégration du système** active le système de protection. Pour modifier cette option, appuyez sur F5 pour ouvrir la fenêtre Configuration avancée, puis cliquez sur > **Protection des documents** dans la configuration avancée complète.

- Reportez-vous à la section Paramètres Threatsense pour plus d'informations sur les paramètres de protection de document.

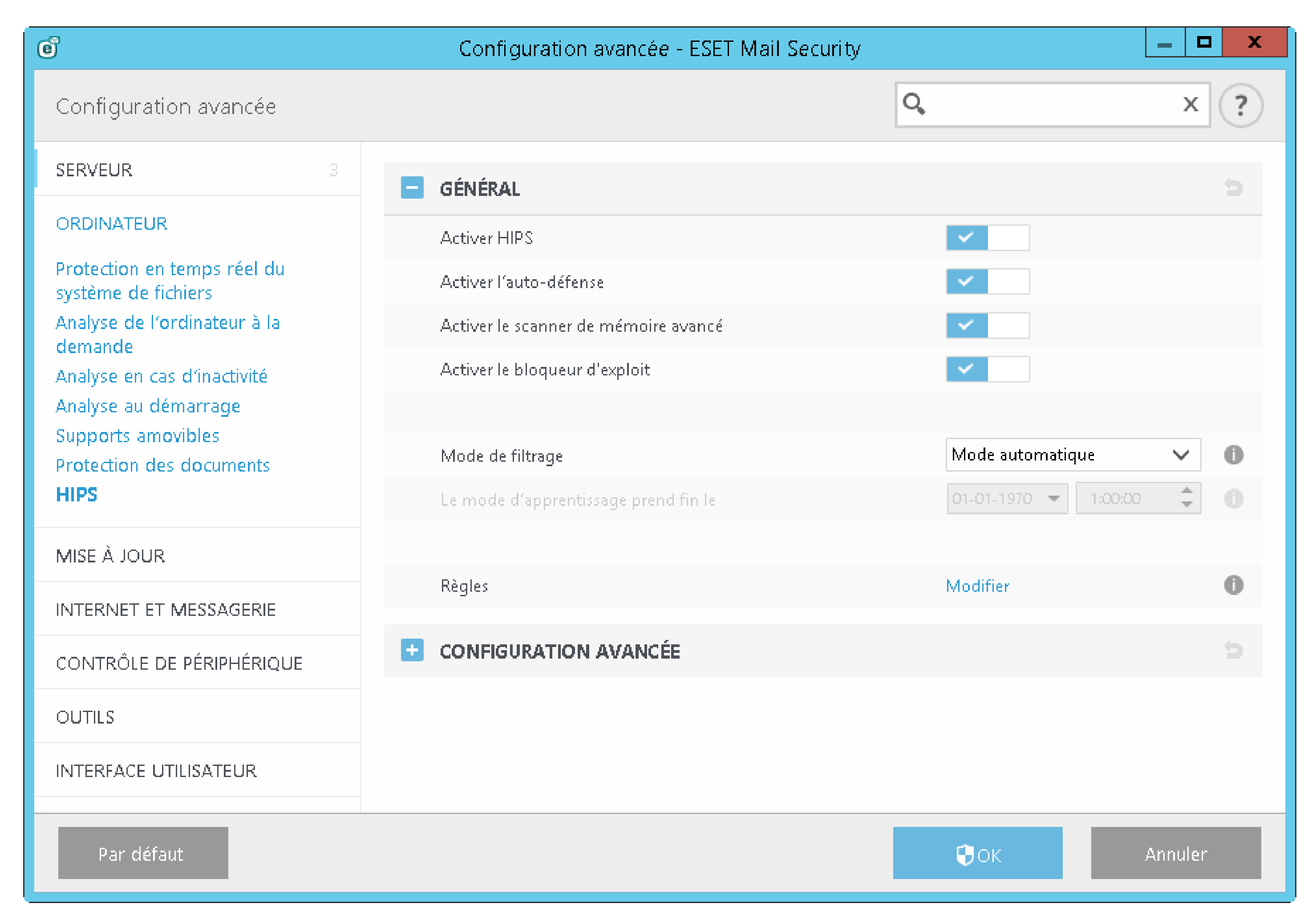
Cette fonctionnalité est activée par des applications utilisant Microsoft Antivirus API (par exemple Microsoft Office 2000 et versions ultérieures, ou Microsoft Internet Explorer 5.0 et versions ultérieures).

5.2.12 HIPS

Les modifications apportées aux paramètres HIPS ne doivent être effectuées que par un utilisateur expérimenté. Une configuration incorrecte des paramètres HIPS peut en effet entraîner une instabilité du système.

Le **système HIPS (Host Intrusion Prevention System)** protège votre système des logiciels malveillants et de toute activité non souhaitée qui pourrait avoir une incidence sur votre ordinateur. Il utilise l'analyse avancée des comportements, associée aux fonctionnalités de détection du filtre réseau qui surveille les processus en cours, les fichiers et les clés de registre. Le système HIPS diffère de la protection en temps réel du système de fichiers et ce n'est pas un pare-feu. Il surveille uniquement les processus en cours d'exécution au sein du système d'exploitation.

Les paramètres HIPS sont disponibles dans **Configuration avancée** (F5) > > **HIPS**. L'état HIPS (activé/désactivé) est indiqué dans la fenêtre principale ESET Mail Security, dans le volet **Configuration**, dans la partie droite de la section **Ordinateur**.



ESET Mail Security intègre la technologie *Auto-défense* qui empêche les logiciels malveillants d'endommager ou de désactiver la protection antivirus et antispyware ; vous avez la garantie que votre système est protégé en permanence. Les modifications apportées aux paramètres **Activer HIPS** et **Activer l'auto-défense** entrent en vigueur après le redémarrage du système d'exploitation Windows. La désactivation de l'intégralité du système **HIPS** nécessite également un redémarrage de l'ordinateur.

Le **scanner de mémoire avancé** fonctionne avec le bloqueur d'exploit afin de renforcer la protection contre les logiciels malveillants qui ne sont pas détectés par les produits anti-logiciels malveillants grâce à l'obscurcissement ou au chiffrement. Le scanner de mémoire avancé est désactivé par défaut. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Le **bloqueur d'exploit** est conçu pour renforcer les types d'applications connues pour être très vulnérables aux exploits (navigateurs, lecteurs de fichiers PDF, clients de messagerie et composants MS Office). Le bloqueur d'exploit est désactivé par défaut. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Le filtrage peut être effectué dans l'un des quatre modes :

- **Mode automatique** - Les opérations sont autorisées, à l'exception de celles bloquées par des règles prédéfinies qui protègent votre système
- **Mode intelligent** - L'utilisateur n'est averti que lors d'événements très suspects.
- **Mode interactif** - L'utilisateur est invité à confirmer les opérations.
- **Mode basé sur des règles personnalisées** - Les opérations sont bloquées.
- **Mode d'apprentissage** - Les opérations sont autorisées et une règle est créée après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'éditeur de règles, mais leur niveau de priorité est inférieur à celui des règles créées manuellement ou en mode automatique. Lorsque vous sélectionnez l'option Mode d'apprentissage dans le menu déroulant Mode de filtrage HIPS, le paramètre « Le mode d'apprentissage prend fin le » devient disponible. Sélectionnez la durée du mode d'apprentissage. La durée maximale est de 14 jours. Lorsque la durée spécifiée est arrivée à son terme, vous êtes invité à modifier les règles créées par HIPS en mode d'apprentissage. Vous pouvez également choisir un autre mode de filtrage ou continuer à utiliser le mode d'apprentissage.

Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction de règles qui sont semblables à celles utilisées par le pare-feu personnel. Cliquez sur **Modifier** pour ouvrir la fenêtre de gestion des règles HIPS. Cette fenêtre vous permet de sélectionner, de créer, de modifier ou de supprimer des règles. Vous trouverez des informations détaillées sur la création de règles et sur les opérations HIPS au chapitre Modifier la règle.

Si l'action par défaut d'une règle est définie sur Demander, une boîte de dialogue apparaît à chaque déclenchement de la règle. Vous pouvez choisir de **refuser** ou d'**autoriser** l'opération. Si vous ne choisissez aucune action dans la période donnée, une nouvelle action est sélectionnée en fonction des règles.

La boîte de dialogue permet de créer une règle en fonction de toute nouvelle action détectée par le système HIPS, puis de définir les conditions dans lesquelles autoriser ou bloquer cette action. Pour définir les paramètres exacts, cliquez sur **Afficher les options**. Les règles créées de cette manière sont équivalentes aux règles créées manuellement ; la règle créée à partir d'une boîte de dialogue peut être moins spécifique que celle qui a déclenché l'affichage de la boîte de dialogue. En d'autres termes, après la création d'une règle, la même opération peut déclencher la même fenêtre.

Mémoriser temporairement cette action pour ce processus entraîne la mémorisation de l'action (**Autoriser/Bloquer**) à utiliser jusqu'à la modification des règles ou du mode de filtrage, une mise à jour du module HIPS ou le redémarrage du système. À l'issue de l'une de ces trois actions, les règles temporaires seront supprimées.

5.2.12.1 Règles HIPS

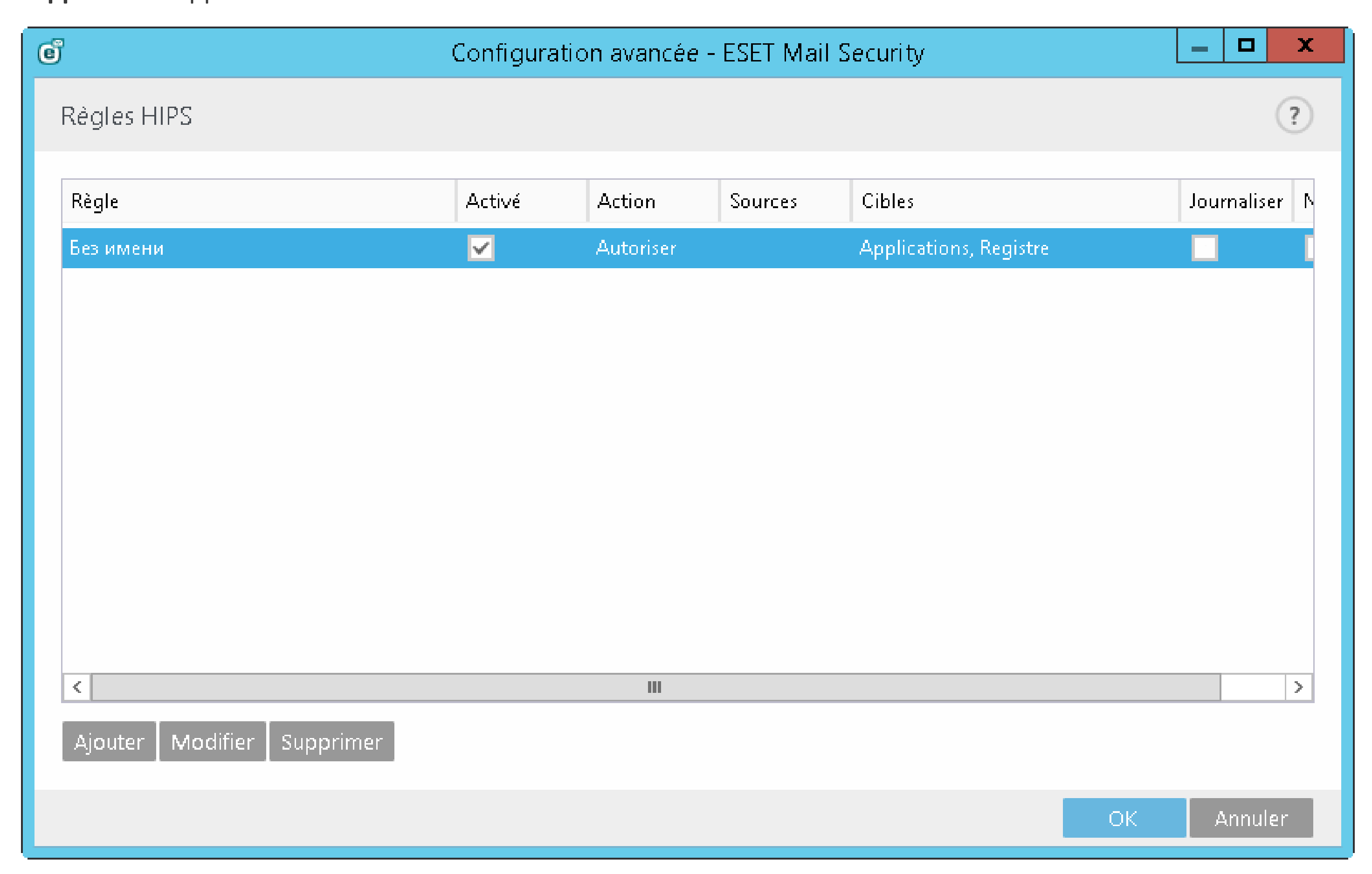
Cette fenêtre vous donne une vue d'ensemble des règles HIPS existantes.

Colonnes

Règle - Nom de règle défini par l'utilisateur ou sélectionné automatiquement.
Activé - Désactivez ce bouton bascule si vous souhaitez conserver la règle dans la liste, mais ne souhaitez pas l'utiliser.
Action - La règle spécifie une action (**Autoriser**, **Bloquer** ou **Demander**) à exécuter, si les conditions sont remplies.
Sources - La règle est utilisée uniquement si l'événement est déclenché par une ou des applications.
Cibles - La règle est utilisée uniquement si l'opération est liée à un fichier, une application ou une entrée de registre spécifique.
Journaliser - Si vous activez cette option, les informations sur cette règle sont écrites dans le journal HIPS.
Notifier - Une petite fenêtre contextuelle apparaît dans le coin inférieur droit si un événement est déclenché.

Éléments de commande

Ajouter - Permet de créer une règle.
Modifier - Permet de modifier des entrées sélectionnées.
Supprimer - Supprime les entrées sélectionnées.



5.2.12.1.1 Paramètres de règle HIPS

- **Nom de règle** - Nom de règle défini par l'utilisateur ou sélectionné automatiquement.
- **Action** - La règle spécifie une action (**Autoriser**, **Bloquer** ou **Demander**) à exécuter, si les conditions sont remplies.
- **Opérations affectant** - Vous devez sélectionner le type d'opération auquel s'applique la règle. La règle est utilisée uniquement pour ce type d'opération et pour la cible sélectionnée.
- **Fichiers** - La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez Fichiers spécifiques, puis cliquez sur Ajouter pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner Tous les fichiers dans le menu déroulant pour ajouter toutes les applications.
- **Applications source** - La règle est utilisée uniquement si l'événement est déclenché par ces applications. Dans le menu déroulant, sélectionnez Applications spécifiques, puis cliquez sur Ajouter pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner Toutes les applications dans le menu déroulant pour ajouter toutes les applications.
- **Entrées du Registre** - La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez Entrées spécifiques, puis cliquez sur Ajouter pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner Toutes les entrées dans le menu déroulant pour ajouter toutes les applications.
- **Activé** - Désactivez ce bouton bascule si vous souhaitez conserver la règle dans la liste, mais ne souhaitez pas l'utiliser.
- **Journaliser** - Si vous activez cette option, les informations sur cette règle sont écrites dans le journal HIPS.
- **Avertir l'utilisateur** - Une petite fenêtre contextuelle apparaît dans l'angle inférieur droit si un événement est déclenché.

La règle se compose de parties qui décrivent les conditions de déclenchement de cette règle :

Applications source - La règle est utilisée uniquement si l'événement est déclenché par cette/ces application(s). Dans le menu déroulant, sélectionnez **Applications spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les applications** dans le menu déroulant pour ajouter toutes les applications.

Fichiers - La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Fichiers spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Tous les fichiers** dans le menu déroulant pour ajouter toutes les applications.

Applications - La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Applications spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les applications** dans le menu déroulant pour ajouter toutes les applications.

Entrées du Registre - La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Entrées spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les entrées** dans le menu déroulant pour ajouter toutes les applications.

Description des opérations importantes :

Opérations sur le fichier

- **Supprimer le fichier** - L'application demande l'autorisation de supprimer le fichier cible.
- **Écrire dans le fichier** - L'application demande l'autorisation d'écrire dans le fichier cible.
- **Accès direct au disque** - L'application essaie de lire des informations du disque ou d'écrire sur le disque d'une manière inhabituelle, non conforme aux procédures Windows classiques. Les fichiers peuvent être modifiés sans que les règles correspondantes soient appliquées. Cette opération peut provenir d'un logiciel malveillant qui essaie de contourner la détection, d'un logiciel de sauvegarde qui tente de faire une copie exacte d'un disque ou encore d'un gestionnaire de partition qui essaie de réorganiser les volumes du disque.
- **Installer l'élément hook global** - Fait référence à l'appel de la fonction SetWindowsHookEx depuis la bibliothèque MSDN.
- **Charger le pilote** - Installation et chargement de pilotes dans le système.

Opérations sur l'application

- **Déboguer une autre application** - Ajout d'un système de débogage au processus. Lors du débogage d'une application, de nombreux détails concernant son comportement peuvent être affichés et modifiés. Vous pouvez également accéder à ses données.
- **Intercepter les événements d'une autre application** - L'application source essaie de récupérer les événements destinés à une application spécifique (il peut s'agir par exemple d'un programme keylogger d'enregistrement des touches qui essaie de capturer les événements d'un navigateur).
- **Arrêter/Mettre en attente une autre application** - Met un processus en attente, le reprend ou l'arrête (accessible directement depuis l'explorateur des processus ou le volet des processus).
- **Démarrer une nouvelle application** - Démarrage de nouvelles applications et de nouveaux processus.
- **Modifier l'état d'une autre application** - L'application source essaie d'écrire dans la mémoire de l'application cible ou d'exécuter du code en son nom. Cette fonctionnalité peut être utile pour protéger une application importante : vous la configurez en tant qu'application cible dans une règle qui bloque l'utilisation de cette opération.

Opérations sur le Registre

- **Modifier les paramètres de démarrage** - Toute modification apportée aux paramètres qui définissent les applications à exécuter au démarrage de Windows. Elles peuvent notamment être recherchées à l'aide de la clé Run du registre Windows.
- **Supprimer du registre** - Suppression d'une clé de registre ou de sa valeur.
- **Renommer la clé de registre** - Changement du nom des clés de registre.
- **Modifier le registre** - Création de nouvelles valeurs de clés de registre, modification de valeurs existantes, déplacement de données dans l'arborescence de base de données ou configuration des droits d'utilisateur ou de groupe pour les clés de registre.

i **REMARQUE :** vous pouvez utiliser des caractères génériques qui peuvent présenter des restrictions lors le la

saisie d'un dossier. Au lieu d'utiliser une clé particulière, vous pouvez utiliser un astérisque (*) dans les chemins de registre. Par exemple *HKEY_USERS*\software* peut vouloir dire *HKEY_USER\.default\software*, mais pas *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** n'est pas un chemin valide de clé de registre. Un chemin de clé de registre contenant le symbole * signifie « ce chemin ou tout autre niveau après ce symbole ». C'est le seul moyen d'utiliser des caractères génériques pour les cibles séjour. L'évaluation porte tout d'abord sur la partie spécifique du chemin, puis sur celle figurant après le symbole (*).

 Si vous créez une règle très générique, l'avertissement concernant ce type de règle s'affiche.

Dans l'exemple suivant, nous allons montrer comment limiter le comportement indésirable des applications :

5.2.12.2 Configuration avancée

Les options suivantes sont utiles au débogage et à l'analyse d'un comportement d'application :

Pilotes dont le chargement est toujours autorisé - Le chargement des pilotes sélectionnés est toujours autorisé, quel que soit le mode de filtrage configuré, excepté en cas de blocage explicite par une règle utilisateur.

Consigner toutes les opérations bloquées - Toutes les opérations bloquées sont inscrites dans le journal HIPS.

Avertir en cas de changements dans les applications de démarrage - Affiche une notification sur le Bureau chaque fois qu'une application est ajoutée au démarrage du système ou en est supprimée.

Veuillez vous reporter à notre base de connaissance pour une version mise à jour de cette page d'aide.

5.2.12.2.1 Pilotes dont le chargement est toujours autorisé

Le chargement des pilotes répertoriés dans cette liste est toujours autorisé quel que soit le mode de filtrage HIPS, sauf s'il est bloqué explicitement par une règle de l'utilisateur.

Ajouter - Ajoute un nouveau pilote.
Modifier - Modifie le chemin d'accès à un pilote sélectionné.
Supprimer - Supprime un pilote de la liste.
Réinitialiser - Recharge un ensemble de pilotes système.

i **REMARQUE :** cliquez sur **Réinitialiser** si vous ne souhaitez pas que les pilotes que vous avez ajoutés manuellement soient inclus. Cette commande peut s'avérer utile lorsque vous avez ajouté plusieurs pilotes et que vous ne pouvez pas les supprimer manuellement de la liste.

5.3 Mettre à jour

Les options de configuration des mises à jour sont accessibles dans l'arborescence **Configuration avancée** (F5), sous **Mise à jour** > **Général**. Cette section permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour utilisés et les données d'authentification donnant accès à ces serveurs.

Général

Le profil de mise à jour en cours d'utilisation est affiché dans le menu déroulant **Profil sélectionné**. Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**, saisissez un nom dans **Nom du profil**, puis cliquez sur **Ajouter**.

En cas de problème de mise à jour, cliquez sur **Effacer** pour effacer le cache de mise à jour temporaire.

Alertes de base des signatures de virus obsolète

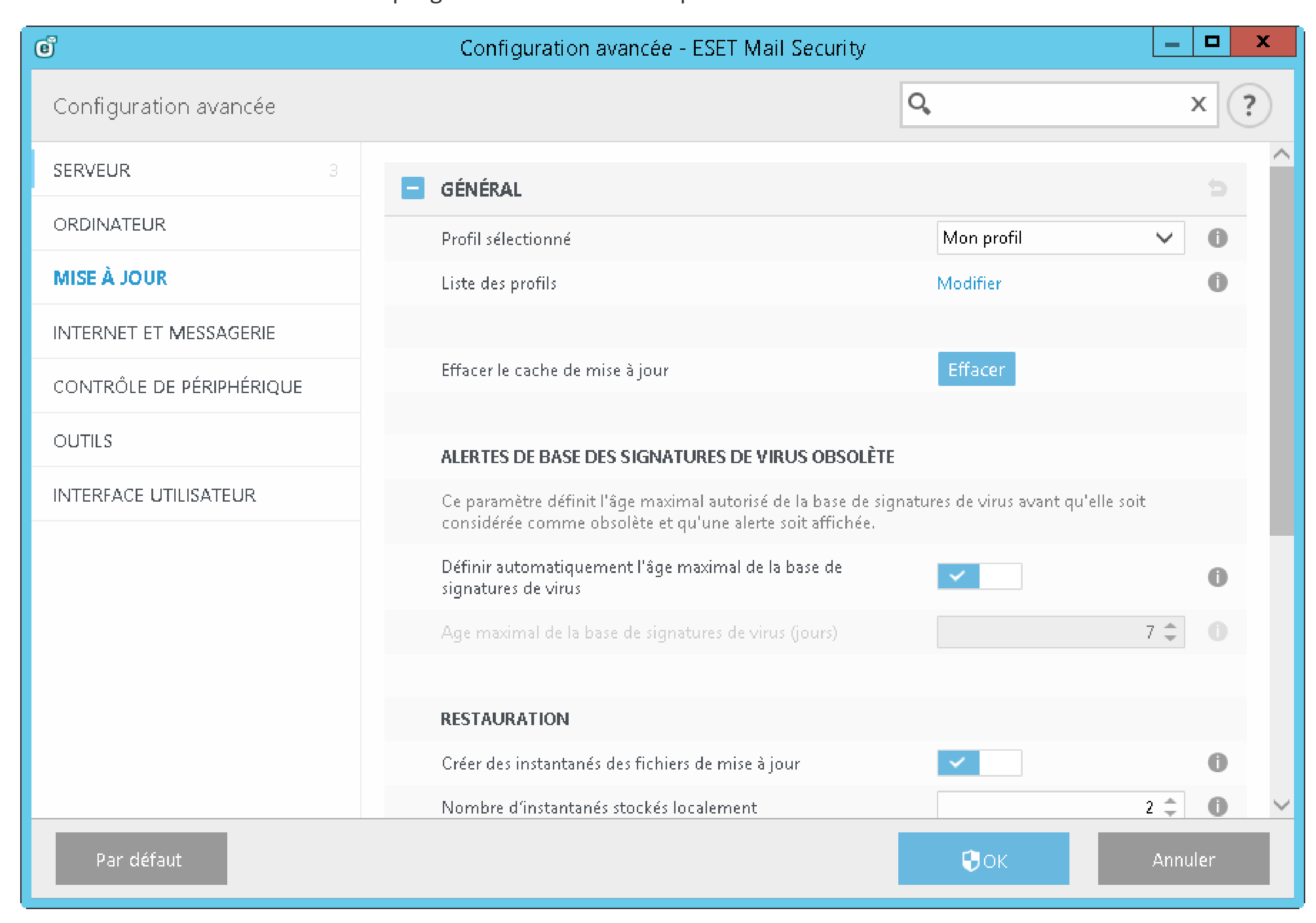
Définir automatiquement l'âge maximal de la base de signatures de virus - Permet de définir la durée maximale (en jours) au terme de laquelle la base des signatures de virus est signalée comme étant obsolète. La valeur par défaut est 7.

Restaurer

Si vous pensez qu'une mise à jour de la base de virus ou des modules du programme est instable ou endommagée, vous pouvez restaurer la version précédente et désactiver les mises à jour pendant une période donnée. Il est également possible d'activer les mises à jour précédemment désactivées si vous les avez reportées pour une durée indéterminée.

ESET Mail Security enregistre des instantanés de base des signatures de virus et de modules du programme à utiliser avec la fonctionnalité de *restauration*. Pour permettre la création d'instantanés de la base de virus, le bouton **Créer des instantanés des fichiers de mise à jour** doit rester activé. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés de la base de virus stockés.

Si vous cliquez sur **Restaurer** (**Configuration avancée** (F5) > **Mise à jour** > **Général**), vous devez sélectionner une durée dans le menu déroulant qui représente la période durant laquelle les mises à jour de la base des signatures de virus et celles des modules de programme sont interrompues.



Il est essentiel de remplir tous les paramètres de mise à jour avec précision afin de télécharger correctement les mises à jour. Si vous utilisez un pare-feu, vérifiez que le programme ESET est autorisé à accéder à Internet (communication HTTP, par exemple).

Par défaut, l'option **Type de mise à jour** (située sous **General**) est définie sur **Mise à jour régulière** pour que les fichiers de mise à jour soient téléchargés automatiquement du serveur ESET lorsque le trafic réseau est le moins surchargé.

General

Désactiver l'affichage d'une notification de réussite de la mise à jour - Désactive les notifications qui apparaissent dans la barre d'état système, dans l'angle inférieur droit de l'écran. Cette option est utile si une application ou un jeu s'exécute en mode plein écran. Veuillez noter que le mode de présentation désactive toutes les notifications.

Le menu **Serveur de mise à jour** est défini par défaut sur SÉLECTION AUTOMATIQUE. Le serveur de mise à jour est l'emplacement où sont stockées les mises à jour. Si vous utilisez un serveur ESET, il est recommandé de conserver

l'option par défaut. Si vous utilisez un serveur de mise à jour personnalisé et souhaitez rétablir le serveur par défaut, saisissez **SÉLECTION AUTOMATIQUE**. ESET Mail Security choisit alors automatiquement les serveurs de mise à jour ESET.

Si un serveur local HTTP, appelé également miroir, est utilisé, le serveur de mise à jour doit être configuré comme suit :
http://nom_ordinateur_ou_son_adresse_IP:2221

Si vous utilisez un serveur local HTTP avec SSL, le serveur de mise à jour doit être configuré comme suit :
https://nom_ordinateur_ou_son_adresse_IP:2221

Si vous utilisez un dossier partagé local, le serveur de mise à jour doit être configuré comme suit :
\\nom_ordinateur_ou_son_adresse_IP\dossier_partagé

Mise à jour à partir du miroir

L'authentification des serveurs de mise à jour est basée sur la **clé de licence** générée et qui vous a été envoyée après l'achat. Lors de l'utilisation d'un serveur miroir local, vous pouvez définir des informations d'identification pour les clients afin qu'ils se connectent au serveur miroir avant la réception des mises à jour. Par défaut, aucune vérification n'est exigée, et les champs **Nom d'utilisateur** et **Mot de passe** restent vides.

5.3.1 Paramètres avancés de mises à jour

Si vous cliquez sur **Restaurer** (**Configuration avancée** (F5) > **Mise à jour** > **Profil**), vous devez sélectionner une durée dans le menu déroulant qui représente la période durant laquelle les mises à jour de la base des signatures de virus et celles des modules de programme sont interrompues.

Sélectionnez **Jusqu'à son retrait** pour différer indéfiniment les mises à jour régulières jusqu'à ce que vous restauriez manuellement cette fonctionnalité. Nous ne recommandons pas de sélectionner cette option qui présente un risque potentiel pour la sécurité de l'ordinateur.

La base des signatures de virus revient à la version la plus ancienne disponible, stockée sous forme d'instantané dans le système de fichiers de l'ordinateur local.

Exemple : admettons que le numéro 10646 correspond à la base des signatures de virus la plus récente. Les bases des signatures de virus 10645 et 10643 sont stockées sous forme d'instantanés. Notez que la base numéro 10644 n'est pas disponible, par exemple parce que l'ordinateur était éteint et qu'une mise à jour plus récente a été mise à disposition avant le téléchargement de la base 10644. Si le champ **Nombre d'instantanés stockés localement** est défini sur 2 et que vous cliquez sur **Restaurer**, la base des signatures de virus (y compris les modules du programme) est restaurée à la version numéro 10643. Ce processus peut prendre un certain temps. Vérifiez si la base des signatures de virus est bien retournée à une version antérieure dans la fenêtre principale de ESET Mail Security, dans la section Mise à jour.

5.3.2 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour des composants du programme. Le programme vous permet de prédéfinir son comportement lorsqu'une nouvelle mise à niveau de composant programme est disponible.

Les mises à jour des composants du programme offrent de nouvelles fonctionnalités ou modifient les versions précédentes. Cette mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme. Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Demander avant de télécharger les composants du programme** - Option par défaut. Vous êtes invité à confirmer ou à refuser les mises à jour de composants de programme lorsqu'elles sont disponibles.
- **Toujours mise à jour les composants du programme** - Les mises à jour de composants du programme sont téléchargées et installées automatiquement. Notez que le redémarrage du système peut être nécessaire.
- **Ne jamais mise à jour les composants du programme** - Aucune mise à jour des composants du programme n'a lieu. Cette option convient aux serveurs, car ces derniers ne peuvent généralement être redémarrés qu'en cas de maintenance.

i **REMARQUE :** la sélection de l'option la plus appropriée dépend du poste de travail sur lequel les paramètres sont appliqués. Notez qu'il existe des différences entre les postes de travail et les serveurs. Par exemple, le redémarrage automatique d'un serveur après une mise à jour du programme peut causer de sérieux dommages.

Si l'option **Demander avant de télécharger une mise à jour** est activée, une notification s'affiche lorsqu'une nouvelle mise à jour est disponible.

Si la taille du fichier de mise à jour est supérieure à la valeur spécifiée dans le champ **Demander si un fichier de mise à jour a une taille supérieure à (Ko)**, le programme affiche une notification.

5.3.3 Proxy HTTP

Pour accéder aux options de configuration du serveur proxy pour un profil de mise à jour donné, cliquez sur **Mise à jour** dans l'arborescence **Configuration avancée** (F5), puis sur **Proxy HTTP**. Cliquez sur le menu déroulant **Mode proxy** et sélectionnez l'une des trois options suivantes :

- Ne pas utiliser de serveur proxy
- Connexion via un serveur proxy
- Utiliser les paramètres globaux de serveur proxy

L'option **Utiliser les paramètres globaux de serveur proxy** utilise les options de configuration de serveur proxy déjà indiquées dans la branche **Outils** > **Serveur proxy** de la configuration avancée complète.

Sélectionnez **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour d'ESET Mail Security.

L'option **Connexion via un serveur proxy** doit être sélectionnée dans les cas suivants :

- Un serveur proxy doit être utilisé pour mettre à jour ESET Mail Security et ce serveur doit être différent de celui indiqué dans les paramètres globaux (**Outils** > **Serveur proxy**). Si c'est le cas, des paramètres supplémentaires doivent être spécifiés : l'adresse du **serveur proxy**, le **port** de communication (3128 par défaut), ainsi que le **nom d'utilisateur** et le **mot de passe** du serveur proxy si nécessaire.
- Les paramètres de serveur proxy n'ont pas été définis globalement, mais ESET Mail Security se connecte à un serveur proxy pour les mises à jour.
- Votre ordinateur est connecté à Internet par l'intermédiaire d'un serveur proxy. Les paramètres sont pris dans Internet Explorer pendant l'installation du programme, mais s'ils sont modifiés par la suite (par exemple, en cas de changement de fournisseur de services Internet), vérifiez que les paramètres du proxy HTTP figurant dans la fenêtre sont corrects. Dans le cas contraire, le programme ne pourra pas se connecter aux serveurs de mise à jour.

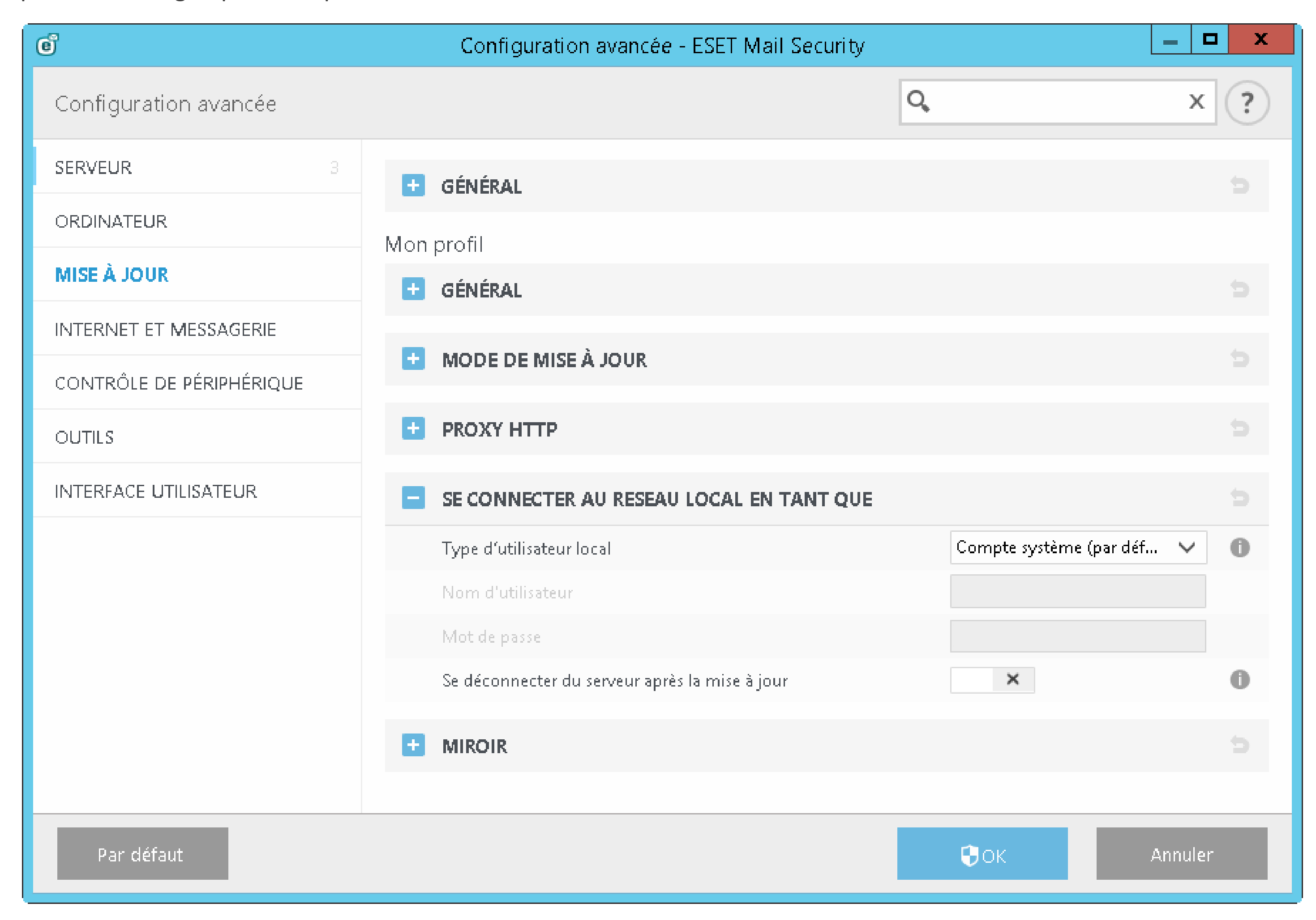
L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

i **REMARQUE :** les données d'authentification telles que **Nom d'utilisateur** et **Mot de passe** permettent d'accéder

au serveur proxy. Ne remplissez ces champs que si un nom d'utilisateur et un mot de passe sont requis. Notez que ces champs ne sont pas ceux du mot de passe/nom d'utilisateur d'ESET Mail Security et ne doivent être remplis que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet via un serveur proxy.

5.3.4 Se connecter au reseau local en tant que

Lors de la mise à jour depuis un serveur local sur un système d'exploitation Windows NT, une authentification est par défaut exigée pour chaque connexion réseau.



Pour configurer un compte de ce type, sélectionnez **Type d'utilisateur local** dans le menu déroulant :

- **Compte système (par défaut)**
- **Utilisateur actuel**
- **Utilisateur spécifié**

Sélectionnez **Compte système (par défaut)** afin d'utiliser le compte système pour l'authentification. Normalement, aucun traitement d'authentification n'a lieu si les données d'authentification ne sont pas fournies dans la section de configuration des mises à jour.

Pour s'assurer que le programme s'authentifie à l'aide du compte de l'utilisateur connecté, sélectionnez **Utilisateur actuel**. L'inconvénient de cette solution est que le programme ne peut pas se connecter au serveur de mise à jour si aucun utilisateur n'est connecté.

Sélectionnez **Utilisateur spécifié** si vous voulez que le programme utilise un compte utilisateur spécifié pour l'authentification. Utilisez cette méthode en cas d'échec de la connexion avec le compte système. Notez que le compte de l'utilisateur spécifié doit avoir accès au dossier des fichiers de mise à jour du serveur local. Dans le cas contraire, le programme serait incapable d'établir une connexion et télécharger les mises à jour.

Avertissement: Si l'une des options **Utilisateur actuel** ou **Utilisateur spécifié** est activée, une erreur peut se produire en cas de changement de l'identité du programme pour l'utilisateur souhaité. C'est pour cette raison que nous recommandons d'entrer les données d'authentification du réseau local dans la section de configuration des mises à

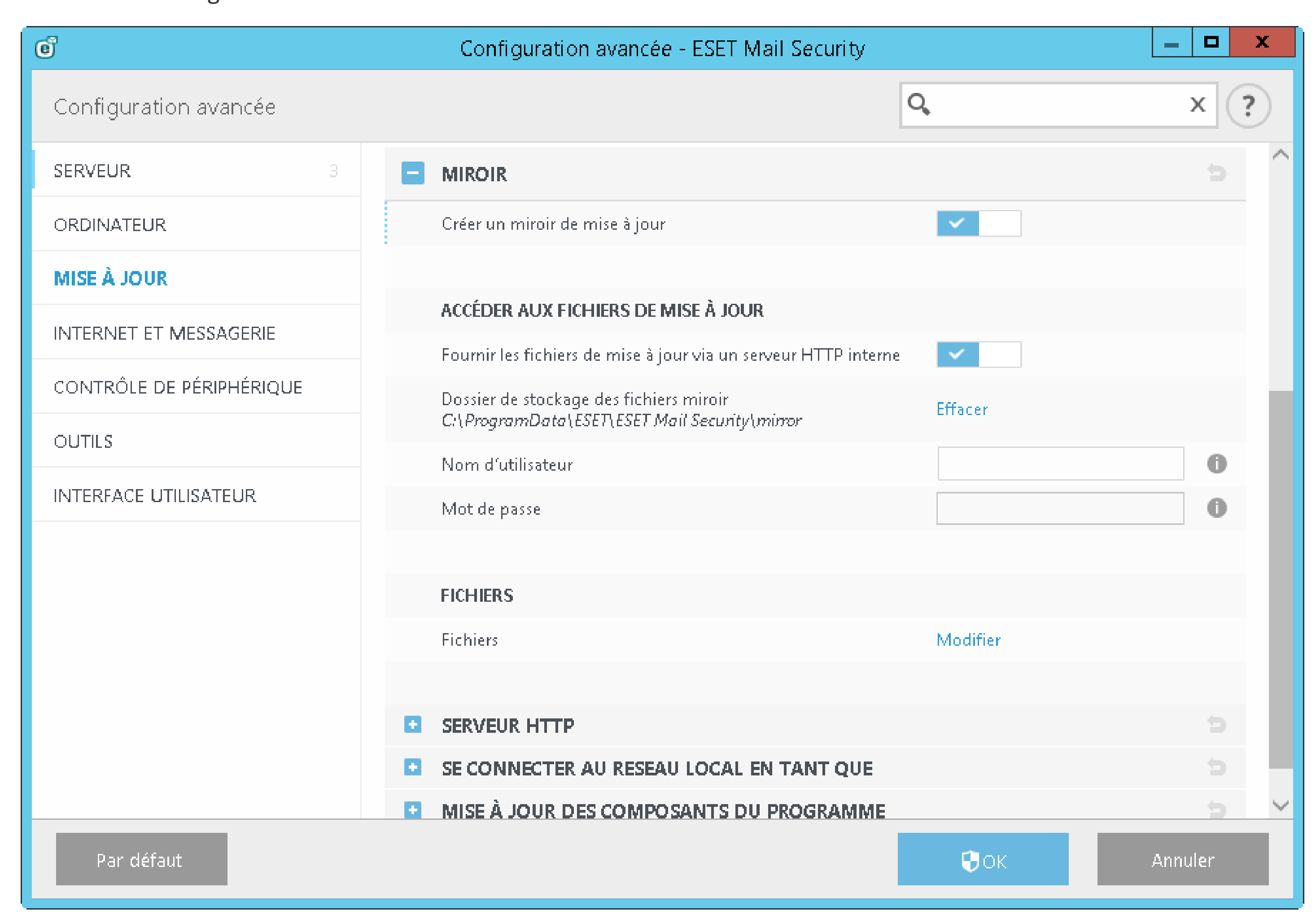
jour. Dans cette section de configuration des mises à jour, les données d'authentification doivent être entrées comme suit : *nom_de_domaine\utilisateur* (dans le cas d'un groupe de travail, entrez *nom_de_groupe_de_travail \utilisateur*) et le mot de passe. La mise à jour de la version HTTP du serveur local n'exige aucune authentification.

Sélectionnez **Déconnecter du serveur après la mise à jour** pour forcer une déconnexion si la connexion au serveur reste active, même après le téléchargement des mises à jour.

5.3.5 Miroir

ESET Mail Security permet de créer des copies des fichiers de mises à jour afin de les utiliser pour la mise à jour d'autres postes de travail du réseau. L'utilisation d'un *miroir*, copie des fichiers de mise à jour dans l'environnement du réseau local, s'avère pratique puisque les fichiers de mise à jour doivent être téléchargés du serveur de mise à jour du fournisseur de manière répétée, pour toutes les stations de travail. Les mises à jour sont téléchargées sur le serveur miroir local puis distribuées à toutes les stations de travail pour éviter tout risque de surcharge du réseau. La mise à jour de postes de travail à partir d'un miroir optimise l'équilibre de la charge réseau et libère les bandes passantes des connexions Internet.

Les options de configuration du serveur miroir local figurent dans Configuration avancée, sous **Mise à jour**. Pour accéder à cette section, appuyez sur F5 (pour ouvrir la fenêtre Configuration avancée), cliquez sur **Mise à jour** et sélectionnez l'onglet **Miroir**.



Pour créer un miroir sur un poste de travail client, activez l'option **Créer un miroir de mise à jour**. L'activation de cette option active d'autres options de configuration du miroir, telles que la manière d'accéder aux fichiers de mise à jour et le chemin des fichiers miroir.

Accéder aux fichiers de mise à jour

Fournir les fichiers de mise à jour via un serveur HTTP interne - Si cette option est activée, les fichiers de mise à jour sont accessibles via un serveur HTTP. Aucune information d'identification n'est requise.

REMARQUE : Windows XP requiert le Service Pack 2 ou une version ultérieure pour utiliser le serveur HTTP.

Les méthodes d'accès au serveur miroir sont décrites en détail dans Mise à jour à partir du miroir. Il existe deux méthodes de base pour accéder au miroir : le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou les clients peuvent accéder au miroir situé sur un serveur HTTP.

Le dossier dédié aux fichiers de mise à jour du miroir peut être défini sous **Dossier de stockage des fichiers miroir**. Cliquez sur **Dossier** pour naviguer jusqu'au dossier souhaité sur un ordinateur local ou un dossier réseau partagé. Si une autorisation pour le dossier spécifié est requise, les données d'authentification doivent être entrées dans les champs **Nom d'utilisateur** et **Mot de passe**. Si le dossier de destination sélectionné se trouve sur un disque réseau exécutant le système d'exploitation Windows NT/2000/XP, le nom d'utilisateur et le mot de passe spécifiés doivent disposer du droit d'écriture sur ce dossier. Le nom d'utilisateur et le mot de passe doivent être entrés au format *Domaine/Utilisateur* ou *Groupe de travail/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Fichiers - Lors de la configuration du miroir, vous pouvez indiquer les versions linguistiques des mises à jour à télécharger. Les langues sélectionnées doivent être prises en charge par le serveur miroir configuré par l'utilisateur.

Serveur HTTP

Port du serveur - Par défaut, le port du serveur est défini sur 2221.

Authentification - Définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **Aucune**, **General** et **NTLM**. Sélectionnez **General** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe. L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour est utilisé pour l'authentification. L'option par défaut est **AUCUNE**. Elle autorise l'accès aux fichiers des mises à jour sans exiger d'authentification.

Ajoutez votre **fichier de chaîne de certificat** ou générez un certificat signé automatiquement si vous souhaitez exécuter le serveur HTTP avec la prise en charge HTTPS (SSL). Les types de certificats suivants sont disponibles : ASN, PEM et PFX. Pour plus de sécurité, vous pouvez utiliser le protocole HTTPS pour télécharger les fichiers de mise à jour. Il est pratiquement impossible d'identifier des transferts de données et des informations de connexion lorsque ce protocole est utilisé. L'option **Type de clé privée** est définie sur **Intégrée** par défaut (ainsi, l'option **Fichier de clé privée** est désactivée par défaut), ce qui signifie que la clé privée fait partie du fichier de chaîne de certificat sélectionné.

Se connecter au réseau local comme

Type d'utilisateur local - Les paramètres **Compte système (par défaut)**, **Utilisateur actuel** et **Utilisateur spécifié** s'affichent dans les menus déroulants correspondants. Les paramètres **Nom d'utilisateur** et **Mot de passe** sont facultatifs. Voir Se connecter au réseau local comme.

Sélectionnez **Déconnecter du serveur après la mise à jour** pour forcer une déconnexion si la connexion au serveur reste active, même après le téléchargement des mises à jour.

Mise à jour des composants du programme

Mettre à jour automatiquement les composants - Permet l'installation de nouvelles fonctionnalités et de mises à jour des fonctionnalités existantes. Une mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme.

Mettre à jour les composants maintenant - Met à jour les composants du programme avec la nouvelle version.

5.3.5.1 Mise à jour à partir du miroir

Il existe deux méthodes de base pour configurer un miroir, qui consiste essentiellement en un référentiel dans lequel les clients peuvent télécharger les fichiers de mise à jour. Le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou un serveur HTTP.

Accès au miroir au moyen d'un serveur HTTP interne

Cette configuration est l'option par défaut ; elle est indiquée dans la configuration du programme prédéfinie. Pour permettre l'accès au miroir à l'aide du serveur HTTP, accédez à **Configuration avancée** >**Mise à jour** > **Miroir**, puis sélectionnez l'option **Créer un miroir de mise à jour**.

Dans la section **Serveur HTTP** de l'onglet **Miroir**, vous pouvez indiquer le **port du serveur** sur lequel le serveur HTTP écoute, ainsi que le type d'**authentification** utilisé par le serveur HTTP. Par défaut, cette option est configurée sur **2221**. L'option **Authentification** définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **Aucune**, **General** et **NTLM**.

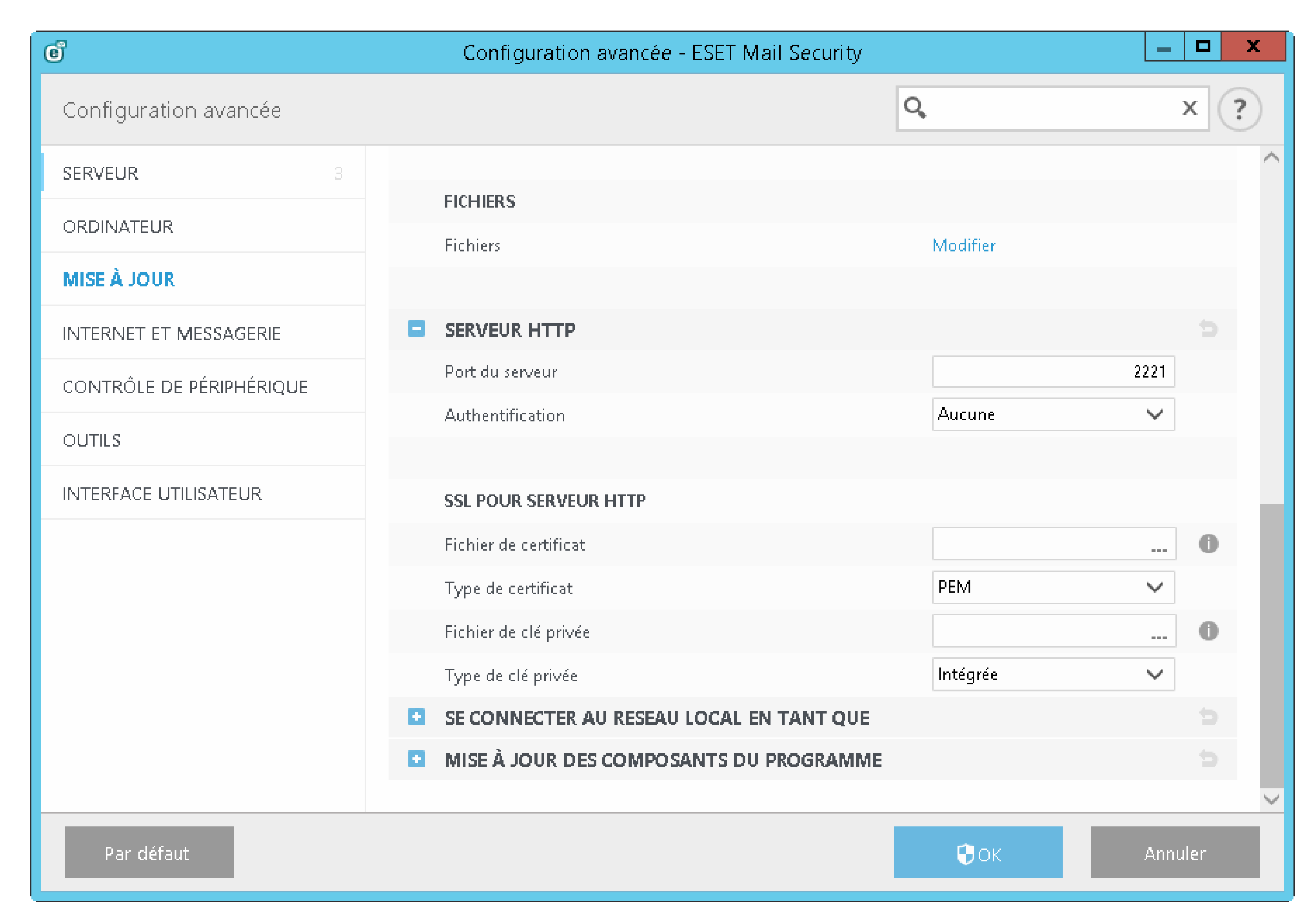
- Sélectionnez **General** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe.
- L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour est utilisé pour l'authentification.
- L'option par défaut est **Aucune**. Elle autorise l'accès aux fichiers des mises à jour sans exiger d'authentification.

Avertissement : l'accès aux fichiers des mises à jour au moyen du serveur HTTP exige que le dossier miroir soit sur le même ordinateur que l'instance ESET Mail Security qui l'a créé.

SSL pour serveur HTTP

Ajoutez votre **fichier de chaîne de certificat** ou générez un certificat signé automatiquement si vous souhaitez exécuter le serveur HTTP avec la prise en charge HTTPS (SSL). Les types de certificats suivants sont disponibles : **PEM, PFX** et **ASN**. Pour plus de sécurité, vous pouvez utiliser le protocole HTTPS pour télécharger les fichiers de mise à jour. Il est pratiquement impossible d'identifier des transferts de données et des informations de connexion lorsque ce protocole est utilisé. L'option **Type de clé privée** est définie par défaut sur **Intégrée**, ce qui signifie que la clé privée fait partie du fichier de chaîne de certificat sélectionné.

i **REMARQUE** : l'erreur **Nom d'utilisateur et/ou mot de passe incorrects** s'affiche dans le volet Mise à jour du menu principal après plusieurs échecs de la mise à jour de la base des signatures de virus à partir du miroir. Il est conseillé d'accéder à **Configuration avancée** > **Mise à jour** > **Miroir** pour vérifier le nom d'utilisateur et le mot de passe. La saisie de données d'authentification incorrectes est raison la plus courante de cette erreur.



Une fois le serveur miroir configuré, vous devez ajouter le nouveau serveur de mise à jour sur les postes de travail clients. Pour ce faire, procédez comme suit :

- Accédez à **Configuration avancée** (F5), puis cliquez sur **Mise à jour** > **General**.
- Désactivez l'option **Choisir automatiquement**, puis ajoutez un nouveau serveur dans le champ **Serveur de mise à jour** dans l'un des formats suivants :
  http://adresse_IP_de_votre_serveur:2221
  https://adresse_IP_de_votre_serveur:2221 (si vous utilisez SSL)

Accès au miroir via le partage des systèmes

Un dossier partagé doit d'abord être créé sur un lecteur local ou réseau. Lors de la création du dossier pour le miroir, il est nécessaire d'octroyer le droit d'*écriture* à l'utilisateur qui va sauvegarder les fichiers de mise à jour dans le dossier et le droit de *lecture* aux utilisateurs qui vont utiliser le dossier miroir pour la mise à jour de ESET Mail Security.

Configurez ensuite l'accès au miroir dans l'onglet **Configuration avancée** > **Mise à jour** > **Miroir** en désactivant l'option **Fournir les fichiers de mise à jour via un serveur HTTP interne**. Cette option est activée par défaut lors de l'installation du programme.

Si le dossier partagé se trouve sur un autre ordinateur du réseau, une authentification est nécessaire pour accéder à l'autre ordinateur. Pour entrer les données d'authentification, ouvrez la **Configuration avancée** de ESET Mail Security (F5) et cliquez sur **Mise à jour** > **Se connecter au réseau local comme**. Il s'agit du même paramètre utilisé pour la mise à jour, comme l'indique la section Se connecter au réseau local comme.

Une fois la configuration du miroir terminée, définissez sur les postes de travail clients *UNC\CHEMIN* comme serveur de mise à jour en procédant comme suit :

1. Ouvrez la **Configuration avancée** de ESET Mail Security et cliquez sur **Mise à jour** > **General**.
2. Cliquez sur **Serveur de mise à jour** et ajoutez un nouveau serveur au format *UNC\PATH*.

i **REMARQUE**: pour que les mises à jour fonctionnent correctement, le chemin du dossier miroir doit être spécifié

comme un chemin UNC. Les mises à jour à partir de lecteurs mappés peuvent ne pas fonctionner.

La dernière section contrôle les composants du programme. Par défaut, les composants de programme téléchargés sont préparés pour copie sur le miroir local. Si l'option **Mettre à jour les composants du programme** est activée, il n'est pas nécessaire de cliquer sur **Mettre à jour** puisque les fichiers sont copiés automatiquement sur le miroir local lorsqu'ils sont disponibles. Voir Mode de mise à jour pour plus d'informations sur les mises à jour des composants du programme.

5.3.5.2 Fichiers miroir

Liste des fichiers de composants de programme disponibles et localisés.

5.3.5.3 Dépannage des problèmes de miroir de mise à jour

Dans la plupart des cas, les problèmes de mise à jour depuis un serveur miroir proviennent des raisons suivantes : mauvaise spécification des options du dossier miroir, données d'authentification incorrectes pour l'accès au dossier miroir, mauvaise configuration des postes de travail qui cherchent à télécharger des fichiers de mise à jour du miroir ou combinaison des raisons citées précédemment. Nous donnons ici un aperçu des problèmes les plus fréquents qui peuvent se produire lors d'une mise à jour depuis le miroir :

- **ESET Mail Security signale une erreur de connexion au serveur miroir** - probablement causée par une spécification incorrecte du serveur de mise à jour (chemin réseau du dossier miroir) à partir duquel les postes de travail locaux téléchargent les mises à jour. Pour vérifier le dossier, cliquez sur le menu **Démarrer** de Windows, puis sur **Exécuter**, entrez le nom du dossier et cliquez sur **OK**. Le contenu du dossier doit s'afficher.

- **ESET Mail Security exige un nom d'utilisateur et un mot de passe** : l'erreur est probablement causée par l'entrée dans la section mise à jour de données d'authentification incorrectes (Nom d'utilisateur et Mot de passe). Le nom d'utilisateur et le mot de passe donnent accès au serveur de mise à jour, à partir duquel le programme se télécharge. Assurez-vous que les données d'authentification sont correctes et entrées dans le bon format. Par exemple, *Domaine/Nom d'utilisateur* ou *Groupe de travail/Nom d'utilisateur*, en plus des mots de passe correspondants. Si le serveur miroir est accessible à Tous, cela ne veut pas dire que tout utilisateur est autorisé à y accéder. « Tous » ne veut pas dire tout utilisateur non autorisé, cela veut tout simplement dire que le dossier est accessible à tous les utilisateurs du domaine. Par conséquent, si le dossier est accessible à Tous, un nom d'utilisateur du domaine et un mot de passe sont toujours nécessaires et doivent être entrés dans la configuration des mises à jour.

- **ESET Mail Security signale une erreur de connexion au serveur miroir** – le port de communication défini pour l'accès au miroir via HTTP est bloqué.

5.3.6 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mise à jour la base des signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur **Mise à jour** dans le menu principal.

Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Mail Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion d'accès à distance**
- **Mise à jour automatique après ouverture de session utilisateur**

Chaque tâche de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur du présent guide.

5.4 Internet et messagerie

La section **Internet et messagerie** permet de configurer la protection du client de messagerie, de protéger la communication sur Internet à l'aide de la protection de l'accès au Web et de contrôler les protocoles Internet en configurant le filtrage des protocoles. Ces fonctionnalités sont essentielles à la protection de votre ordinateur lorsqu'il communique par Internet.

La **protection du client de messagerie** contrôle toute la communication par messagerie, protège des codes malveillants et vous permet de choisir l'action à entreprendre en cas de détection d'infection.

La protection de l'accès au Web surveille la communication entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPS. Cette fonctionnalité permet également de bloquer, d'autoriser et d'exclure certaines adresses URL.

Le **filtrage des protocoles** est une protection avancée destinée aux protocoles d'application et fournie par le moteur d'analyse ThreatSense. Ce contrôle fonctionne automatiquement, que le programme utilisé soit un navigateur Internet ou un client de messagerie. Il fonctionne également pour la communication chiffrée (SSL).

5.4.1 Filtrage des protocoles

Filtrage des protocoles

La protection antivirus des protocoles d'application est fournie par le moteur d'analyse ThreatSense qui intègre en toute transparence toutes les techniques avancées d'analyse des logiciels malveillants. Le filtrage des protocoles fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Pour modifier les paramètres chiffrés (SSL), accédez à **Internet et messagerie** > **Contrôle de protocole SSL**.

Activer le filtrage du contenu des protocoles d'application - Cette option peut être utilisée pour désactiver le filtrage des protocoles. Notez que la plupart des composants d'ESET Mail Security (protection de l'accès Web, protection des protocoles de messagerie et protection antihameçonnage) dépendent de ce filtrage et ne fonctionneront pas sans celui-ci.

Applications exclues - Permet d'exclure du filtrage des protocoles certaines adresses distantes. Cette option s'avère utile lorsque le filtrage des protocoles entraîne des problèmes de compatibilité.

Adresses IP exclues - Permet d'exclure des applications spécifiques du filtrage des protocoles. Cette option s'avère utile lorsque le filtrage des protocoles entraîne des problèmes de compatibilité.

Web et clients de messagerie - Utilisée uniquement sur les systèmes d'exploitation Windows, cette option permet de sélectionner les applications pour lesquelles tout le trafic est filtré par le filtrage des protocoles, indépendamment des ports utilisés.

Enregistrer les informations nécessaires pour que l'assistance ESET puisse diagnostiquer les problèmes de filtrage des protocoles - Active la journalisation avancée des données de diagnostic. Utilisez cette option uniquement sur demande de l'assistance ESET.

5.4.1.1 Applications exclues

Pour exclure du filtrage de contenu la communication de certaines applications sensibles au réseau, sélectionnez ces applications dans la liste. Aucune recherche de menace n'est effectuée sur la communication HTTP/POP3 des applications sélectionnées. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

Les applications et les services qui ont déjà été affectés par le filtrage des protocoles sont automatiquement affichés après avoir cliqué sur **Ajouter**.

Modifier - Modifie les entrées sélectionnées de la liste.

Supprimer - Supprime les entrées sélectionnées de la liste.

5.4.1.2 Adresses IP exclues

Les adresses IP figurant dans cette liste sont exclues du filtrage du contenu des protocoles. Les menaces ne sont pas détectées sur les communications HTTP/POP3/IMAP liées aux adresses sélectionnées. Il est recommandé d'utiliser cette option uniquement pour les adresses que vous savez être fiables.

Ajouter - Cliquez pour ajouter une adresse IP/une plage d'adresses IP/un sous-réseau d'un point distant auquel une règle est appliquée.

Modifier - Modifie les entrées sélectionnées de la liste.

Supprimer - Supprime les entrées sélectionnées de la liste.

5.4.1.3 Clients Internet et de messagerie

REMARQUE : depuis Windows Vista Service Pack 1 et Windows Server 2008, la nouvelle architecture de plateforme de filtrage Windows permet de vérifier les communications réseau. Étant donné que la technologie WFP utilise des techniques de surveillance spéciales, la section **Internet et clients de messagerie** est indisponible.

À cause du nombre considérable de codes malveillants circulant sur Internet, la sécurisation de la navigation sur Internet est un aspect très important de la protection des ordinateurs. Les vulnérabilités des navigateurs Internet et les liens frauduleux contribuent à faciliter l'accès imperceptible au système par des codes malveillants. C'est pourquoi ESET Mail Security se concentre sur la sécurité des navigateurs Internet. Chaque application accédant au réseau peut être marquée comme étant un navigateur Internet. Les applications qui ont déjà utilisé des protocoles pour les communications ou les applications des chemins d'accès sélectionnés peuvent être ajoutées à la liste Internet et clients de messagerie.

5.4.2 Contrôle de protocole SSL

ESET Mail Security est capable de rechercher les menaces dans les communications qui utilisent le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour examiner les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

Activer le filtrage du protocole SSL - Si le filtrage des protocoles est désactivé, le programme n'analyse pas les communications sur le protocole SSL.

Le **mode de filtrage de protocole SSL** est disponible dans les options suivantes :

- **Mode automatique** - Sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accédez à un serveur disposant d'un certificat non approuvé indiqué comme fiable (il figure dans la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

- **Mode interactif** - Si vous entrez un nouveau site protégé par SSL (avec un certificat inconnu), une boîte de dialogue de sélection d'action s'affiche. Ce mode vous permet de créer la liste des certificats SSL qui seront exclus de l'analyse.

Bloquer les communications chiffrées à l'aide du protocole obsolète SSL v2 - Les communications utilisant la version antérieure du protocole SSL sont automatiquement bloquées.

Certificat racine

Certificat racine : pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET à la liste des certificats racines connus (éditeurs). L'option **Ajouter le certificat racine aux navigateurs connus** doit être activée. Sélectionnez cette option pour ajouter automatiquement le certificat racine d'ESET aux navigateurs connus (Opera et Firefox par exemple). Pour les navigateurs utilisant le magasin de certification système, le certificat est ajouté automatiquement (Internet Explorer par exemple).

Pour appliquer le certificat à des navigateurs non pris en charge, cliquez sur **Afficher le certificat** > **Détails** > **Copier dans un fichier**, puis importez-le manuellement dans le navigateur.

Validité du certificat

S'il est impossible de vérifier le certificat à l'aide du magasin de certificats TRCA : dans certains cas, il est impossible de vérifier le certificat d'un site Web à l'aide du magasin d'Autorités de certification racine de confiance. Cela signifie que le certificat est signé par un utilisateur (l'administrateur d'un serveur Web ou d'une petite entreprise, par exemple) et que le fait de le considérer comme fiable n'est pas toujours un risque. La plupart des grandes entreprises (les banques par exemple) utilisent un certificat signé par TRCA. Si l'option **Interroger sur la validité du certificat** est activée (sélectionnée par défaut), l'utilisateur est invité à sélectionner une action à entreprendre lorsque la communication chiffrée est établie. Vous pouvez sélectionner **Bloquer toute communication utilisant le certificat** pour mettre toujours fin aux connexions chiffrées aux sites avec des certificats non vérifiés.

Si le certificat n'est pas valide ou est endommagé : cela signifie qu'il est arrivé à expiration ou que sa signature est incorrecte. Dans ce cas, il est recommandé de conserver l'option **Bloquer toute communication utilisant le certificat** activée.

La **liste des certificats connus** permet de personnaliser le comportement d'ESET Mail Security pour des certificats SSL spécifiques.

5.4.2.1 Communication SSL chiffrée



Si votre système est configuré pour utiliser l'analyse du protocole SSL, une boîte de dialogue vous invitant à choisir une action peut s'afficher dans les deux cas suivants :

Lorsqu'un site Web utilise un certificat non valide ou ne pouvant pas être vérifié et qu'ESET Mail Security est configuré pour demander à l'utilisateur l'action à effectuer dans ce cas (par défaut, oui pour les certificats ne pouvant pas être vérifiés, non pour les certificats non valides), une boîte de dialogue s'affiche pour **autoriser** ou **bloquer** la connexion.

Lorsque l'option **Mode de filtrage du protocole SSL** est définie sur **Mode interactif**, une boîte de dialogue demande pour chaque site Web d'**analyser** ou d'**ignorer** le trafic. Certaines applications vérifient que le trafic SSL n'est ni modifié ni inspecté par quelqu'un. Dans ce cas, ESET Mail Security doit **ignorer** ce trafic pour que les applications continuent de fonctionner.

Dans les deux cas, l'utilisateur peut choisir de mémoriser l'action sélectionnée. Les actions enregistrées sont stockées dans la **liste des certificats connus**.

5.4.2.2 Liste des certificats connus

La liste des certificats connus peut être utilisée pour personnaliser le comportement d'ESET Mail Security pour des certificats SSL spécifiques et mémoriser les actions choisies en cas de sélection du mode interactif dans le mode de filtrage de protocole SSL. La liste peut être affichée et modifiée dans **Configuration avancée** (F5) > **Internet et messagerie** > **Contrôle de protocole SSL** > **Liste des certificats connus**.

La fenêtre **Liste des certificats connus** contient les éléments suivants :

Colonnes

- **Nom** - Nom du certificat.
- **Émetteur du certificat** - Nom du créateur du certificat.
- **Objet du certificat** - Le champ d'objet identifie l'entité associée à la clé publique stockée dans le champ d'objet de la clé publique.
- **Accès** - Sélectionnez **Autoriser** ou **Bloquer** comme **action d'accès** pour autoriser/bloquer la communication sécurisée par ce certificat, indépendamment de sa fiabilité. Sélectionnez **Automatique** pour autoriser les certificats approuvés et demander quelle action effectuer pour les certificats non approuvés. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.
- **Analyser** - Sélectionnez **Analyser** ou **Ignorer** comme **Action d'analyse** pour analyser ou ignorer les communications sécurisées par ce certificat. Sélectionnez **Automatique** pour effectuer une analyse en mode automatique et demander quelle action entreprendre en mode interactif. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

Éléments de commande

- **Modifier** - Sélectionnez le certificat à configurer, puis cliquez sur **Modifier**.
- **Supprimer** - Sélectionnez le certificat à supprimer, puis cliquez sur **Supprimer**.
- **OK/Annuler** - Cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler** pour quitter sans enregistrer.

5.4.3 Protection du client de messagerie

L'intégration d'ESET Mail Security aux clients de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, l'intégration peut être activée dans ESET Mail Security. Lorsque l'intégration est activée, la barre d'outils d'ESET Mail Security est insérée directement dans le client de messagerie (la barre d'outils pour les nouvelles versions de Windows Live Mail n'est pas insérée), ce qui permet une protection plus efficace des messages. Les paramètres d'intégration sont situés sous **Configuration** > **Configuration avancée** > **Internet et messagerie** > **Protection du client de messagerie** > **Clients de messagerie**.

Intégration aux clients de messagerie

Les clients de messagerie actuellement pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail et Windows Live Mail. Ce module fonctionne comme un plugin pour ces programmes. L'avantage principal du plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie au scanner de virus. Pour obtenir la liste complète des clients de messagerie pris en charge, avec leur version, reportez-vous à cet article de la base de connaissances ESET.

Même si l'intégration n'est pas activée, les communications par messagerie demeurent protégées par le module de protection du client de messagerie (POP3, IMAP).

Activez l'option **Désactiver la vérification au changement de contenu de la boîte aux lettres** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie (MS Outlook uniquement). Ce cas de figure peut survenir lors de la récupération d'un courrier électronique à partir du magasin Kerio Outlook Connector.

Courrier électronique à analyser

Courrier reçu - Active/désactive la vérification des messages reçus.
Courrier envoyé - Active/désactive la vérification des messages envoyés.
Courrier lu - Active/désactive la vérification des messages lus.

Action à exécuter sur le courrier électronique infecté

Aucune action - Si cette option est activée, le programme identifie les pièces jointes infectées, mais n'entreprend aucune action sur les messages concernés.
Supprimer les courriers - Le programme avertit l'utilisateur à propos d'une infiltration et supprime le message.
Déplacer les courriers vers le dossier Éléments supprimés - Les courriers infectés sont automatiquement placés dans le dossier Éléments supprimés.
Déplacer les courriers vers le dossier - Les courriers infectés sont automatiquement placés dans le dossier spécifié.

Dossier - Spécifiez le dossier personnalisé vers lequel les messages infectés doivent être déplacés lorsqu'ils sont détectés.

Répéter l'analyse après mise à jour - Active/désactive la répétition de l'analyse après la mise à jour de la base des signatures de virus.

Accepter les résultats d'analyse d'autres modules - Si cette option est activée, le module de protection de messages accepte les résultats d'analyse d'autres modules de protection (analyse des protocoles IMAP, POP3).

5.4.3.1 Protocoles de messagerie

Les protocoles IMAP et POP3 sont les protocoles les plus répandus pour la réception de messages dans un client de messagerie. ESET Mail Security protège ces protocoles, quel que soit le client de messagerie utilisé, sans qu'il soit nécessaire de reconfigurer le client de messagerie.

Vous pouvez configurer le contrôle des protocoles IMAP/IMAPS et POP3/POP3S dans la configuration avancée. Pour accéder à ce paramètre, développez **Internet et messagerie** > **Protection du client de messagerie** > **Protocoles de messagerie**.

ESET Mail Security prend également en charge l'analyse des protocoles IMAPS et POP3S qui utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Mail Security contrôle la communication à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans les ports utilisés par le protocole IMAPS/POP3S, quelle que soit la version du système d'exploitation.

Les communications chiffrées ne sont pas analysées lorsque les paramètres par défaut sont utilisés. Pour activer l'analyse des communications chiffrées, accédez à l'option Contrôle de protocole SSL dans la configuration avancée, cliquez sur **Internet et messagerie** > **Contrôle de protocole SSL**, puis sélectionnez **Activer le filtrage du protocole SSL**.

5.4.3.2 Alertes et notifications

La protection de la messagerie permet de contrôler les communications reçues via les protocoles POP3 et IMAP. ESET Mail Security utilise le plugin pour Microsoft Outlook et d'autres clients de messagerie pour contrôler toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP). Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées comprises dans le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec la base des signatures de virus. L'analyse des communications via le protocole POP3 et IMAP est indépendante du client de messagerie utilisé.

Les options de cette fonctionnalité sont disponibles dans **Configuration avancée** sous **Internet et messagerie** > **Protection du client de messagerie** > **Alertes et notifications**.

Paramètres ThreatSense - La configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur cette option pour afficher la fenêtre de configuration détaillée de l'analyseur de virus.

Après la vérification d'un courrier, une notification avec le résultat de l'analyse peut être ajoutée au message. Vous pouvez sélectionner **Ajouter une notification aux messages reçus et lus, Ajouter une note à l'objet des messages infectés reçus et lus** ou **Ajouter une notification aux messages envoyés**. Gardez à l'esprit qu'en de rares occasions, les notifications peuvent être omises en cas de messages HTML problématiques ou de messages élaborés par un logiciel malveillant. Les notifications peuvent être ajoutées aux messages reçus et lus, aux messages envoyés, ou aux deux catégories. Les options disponibles sont les suivantes :

- **Jamais** - Aucune notification n'est ajoutée.
- **Aux e-mails infectés seulement** - Seuls les messages contenant un code malveillant sont marqués comme contrôlés (valeur par défaut).
- **Aux e-mails infectés seulement** - Le programme ajoute des messages à tout courrier analysé.

Ajouter une note à l'objet des messages infectés envoyés - Désactivez cette option si vous ne souhaitez pas que la protection de la messagerie ajoute un avertissement de virus dans l'objet d'un message infecté. Cette fonctionnalité permet tout simplement de filtrer les courriers infectés en fonction de son objet (s'il est pris en charge par le programme de messagerie). Elle augmente également la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

Texte ajouté à l'objet des messages infectés - Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un courrier infecté. Cette fonction remplace l'objet du message *"Bonjour"* par le préfixe *"[virus]"* au format suivant : *"[virus] Bonjour"*. La variable *%VIRUSNAME%* représente la menace détectée.

5.4.3.3 Barre d'outils MS Outlook

La protection Microsoft Outlook fonctionne comme un module plugin. Après l'installation d'ESET Mail Security, cette barre d'outils contenant les options de protection antivirus est ajoutée à Microsoft Outlook :

ESET Mail Security - Cliquez sur l'icône pour ouvrir la fenêtre principale du programme ESET Mail Security.

Analyser à nouveau les messages - Vous permet de lancer manuellement la vérification des messages. Vous pouvez indiquer les messages à vérifier et activer une nouvelle analyse du message reçu. Pour plus d'informations, consultez la section Protection du client de messagerie.

Configuration du moteur d'analyse - Affiche les options de configuration de la Protection du client de messagerie.

5.4.3.4 Barre d'outils Outlook Express et Windows Mail

La protection pour Outlook Express et Windows Mail fonctionne comme un module plugin. Après l'installation d'ESET Mail Security, cette barre d'outils contenant les options de protection antivirus est ajoutée à Outlook Express ou à Windows Mail :

ESET Mail Security - Cliquez sur l'icône pour ouvrir la fenêtre principale du programme ESET Mail Security.

Analyser à nouveau les messages - Vous permet de lancer manuellement la vérification des messages. Vous pouvez indiquer les messages à vérifier et activer une nouvelle analyse du message reçu. Pour plus d'informations, consultez la section Protection du client de messagerie.

Configuration du moteur d'analyse - Affiche les options de configuration de la Protection du client de messagerie.

Interface utilisateur

Personnaliser l'apparence - Vous pouvez modifier l'apparence de la barre d'outils pour votre client de messagerie. Désactivez cette option pour personnaliser l'apparence indépendamment des paramètres du programme de messagerie.

Afficher le texte - Affiche des descriptions des icônes.

Texte à droite - Les descriptions d'options sont déplacées du bas vers le côté droit des icônes.

Grandes icônes - Affiche des icônes de grande taille pour les options de menu.

5.4.3.5 Boîte de dialogue de confirmation

Cette notification permet de vérifier que l'utilisateur veut vraiment exécuter l'action sélectionnée, ce qui devrait éliminer des erreurs possibles.

Par ailleurs, la boîte de dialogue offre également la possibilité de désactiver les confirmations.

5.4.3.6 Analyser à nouveau les messages

La barre d'outils d'ESET Mail Security intégrée dans les clients de messagerie permet aux utilisateurs de spécifier plusieurs options pour la vérification du courrier électronique. L'option **Analyser à nouveau les messages** offre deux modes d'analyse :

Tous les messages du dossier en cours - Analyse les messages du dossier affiché.

Messages sélectionnés uniquement - Analyse uniquement les messages marqués par l'utilisateur.

La case à cocher **Réanalyser les messages déjà analysés** permet d'exécuter une autre analyse sur des messages déjà analysés.

5.4.4 Protection de l'accès Web

La connectivité Internet est une fonctionnalité standard sur la plupart des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. La protection de l'accès au Web opère par surveillance des communications entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPS (communications chiffrées).

L'accès aux pages Web connues pour comporter du contenu malveillant est bloqué avant le téléchargement du contenu. Toutes les autres pages Web sont analysées par le moteur d'analyse ThreatSense lors de leur chargement et sont bloquées en cas de détection de contenu malveillant. La protection de l'accès Web offre deux niveaux de protection : un blocage par liste noire et un blocage par contenu.

Il est vivement recommandé de conserver l'option de protection de l'accès Web activée. Cette option est accessible à partir de la fenêtre principale de ESET Mail Security en accédant à **Configuration** > **Internet et messagerie** > **Protection de l'accès Web**.

Les options suivantes sont disponibles dans **Configuration avancée** (F5) > **Internet et messagerie** > **Protection de l'accès Web** :

- **Protocoles Web** - Permet de configurer le contrôle de ces protocoles standard qui sont utilisés par la plupart des navigateurs Internet.
- **Gestion des adresses URL** - Permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification.
- **Configuration des paramètres du moteur ThreatSense** - La configuration avancée de l'analyseur de virus permet de configurer des paramètres tels que les types d'objet à analyser (courriers électroniques, archives, etc.), les méthodes de détection pour la protection de l'accès Web, etc.

5.4.4.1 Gestion d'adresse URL

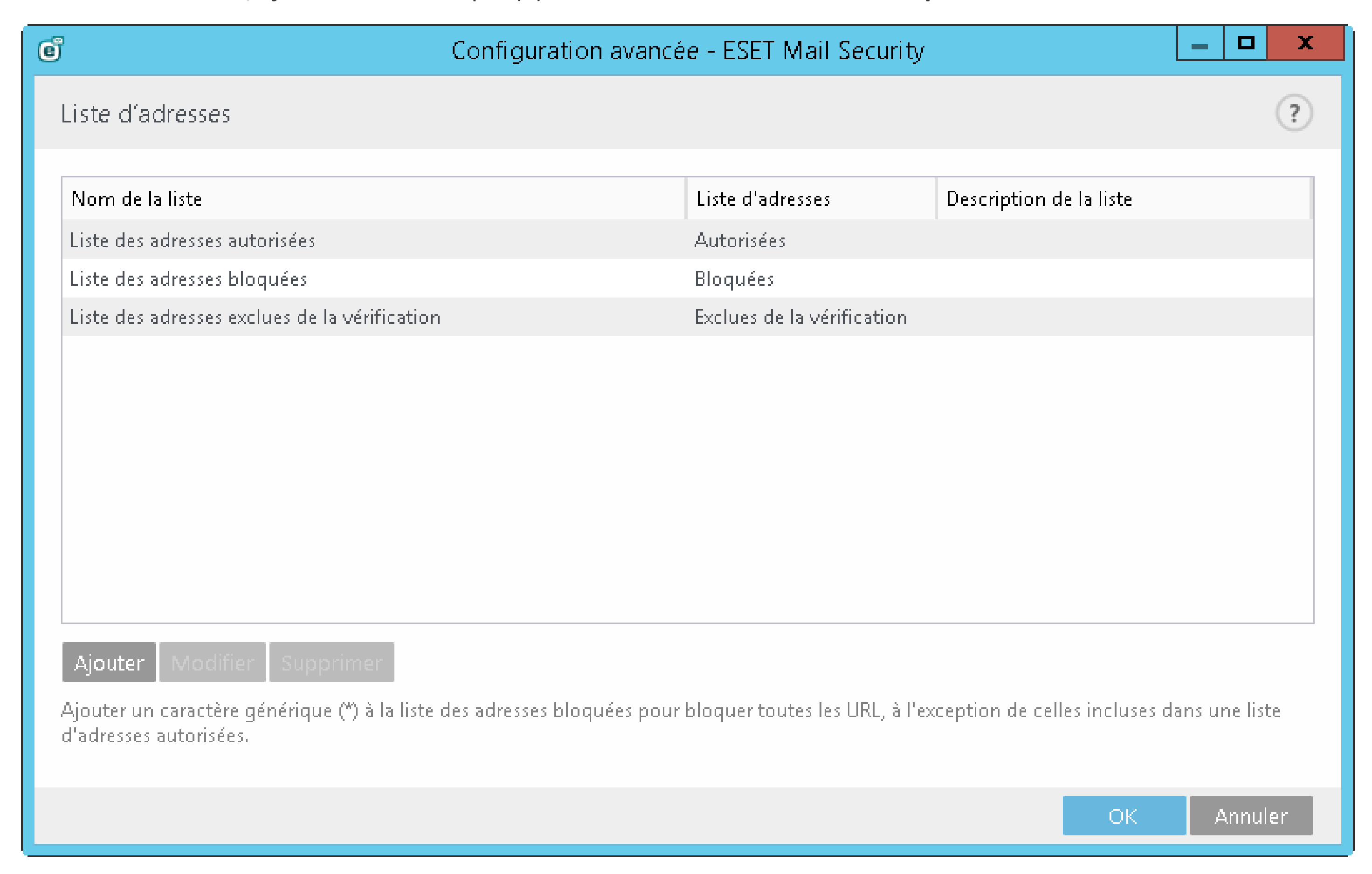
La section Gestion d'adresse URL permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification.

Les sites Web qui figurent dans la liste des adresses bloquées ne sont pas accessibles, sauf s'ils sont également inclus dans la liste des adresses autorisées. Les sites Web qui se trouvent dans la liste des adresses exclues de la vérification ne font pas l'objet d'une analyse de code malveillant lors de leur accès.

L'option **Activer le filtrage du protocole SSL** doit être sélectionnée si vous souhaitez filtrer les adresses HTTPS en plus des pages Web HTTP. Sinon, seuls les domaines des sites HTTPS que vous avez visités sont ajoutés et non l'URL complète.

Dans toutes les listes, vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque représente n'importe quel chiffre ou caractère, alors que le point d'interrogation symbolise un seul caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et fiables. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste.

Si vous souhaitez bloquer toutes les adresses HTTP, à l'exception des adresses figurant dans la **liste active des adresses autorisées**, ajoutez un astérisque (*) à la **liste active des adresses bloquées**.



Ajouter - Permet de créer une autre liste en plus des listes prédéfinies. Cela peut s'avérer utile si vous souhaitez diviser de manière logique des groupes différents d'adresses. Par exemple, une liste d'adresses bloquées peut contenir les adresses d'une liste noire publique externe et une autre liste peut comporter votre propre liste noire, ce qui simplifie la mise à jour de la liste externe tout en conservant la vôtre intacte.
Modifier - Permet de modifier les listes existantes. Utilisez cette option pour ajouter ou supprimer des adresses des listes.
Supprimer - Permet de supprimer une liste existante. Il est possible uniquement de supprimer les listes créées à l'aide de l'option Ajouter et non les listes par défaut.

5.4.4.1.1 Créer une liste

Cette section permet de spécifier des listes d'adresses URL/masques qui seront bloqués, autorisés ou exclus de la vérification.

Lors de la création d'une liste, vous pouvez configurer les options suivantes :

Type de liste d'adresses - Trois types de liste sont disponibles :

- **Liste des adresses exclues de la vérification** - Aucune vérification de la présence de code malveillant n'est effectuée pour les adresses répertoriées dans la liste.
- **Liste des adresses bloquées** - L'utilisateur n'est pas autorisé à accéder aux adresses répertoriées dans cette liste. Cela ne s'applique qu'au protocole HTTP. Les autres protocoles ne sont pas bloqués.
- **Liste des adresses autorisées** - Si l'option N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées est activée et si la liste des adresses bloquées contient un astérisque (correspond à tout), l'utilisateur n'est autorisé à accéder qu'aux adresses répertoriées dans cette liste. Les adresses de cette liste sont autorisées même si elles correspondent aussi aux adresses bloquées.

Nom de liste - Spécifiez le nom de la liste. Ce champ apparaît grisé lors de la modification de l'une des trois listes prédéfinies.

Description de la liste - Tapez une brève description de la liste (facultatif). Ce champ apparaît en grisé lors de la modification de l'une des trois listes prédéfinies.

Pour activer une liste, sélectionnez l'option **Liste active** en regard de celle-ci. Si vous souhaitez être averti lorsqu'une liste est utilisée pour l'évaluation d'un site HTTP visité, sélectionnez **Notifier lors de l'application**. Par exemple, une notification est émise lorsqu'un site Web est bloqué ou autorisé en raison de son inclusion dans la liste des adresses bloquées ou autorisées. La notification contient le nom de la liste dans laquelle figure le site Web spécifié.

Ajouter - Ajoutez une nouvelle adresse URL à la liste (entrez plusieurs valeurs avec un séparateur).

Modifier - Permet de modifier une adresse existante dans la liste. Il est possible de supprimer uniquement les adresses créées à l'aide de l'option Ajouter.

Supprimer - Permet de supprimer des adresses existantes de la liste. Il est possible de supprimer uniquement les adresses créées à l'aide de l'option Ajouter.

Importer - Importez un fichier comportant des adresses URL (séparez les valeurs par un saut de ligne, par exemple *.txt utilisant le codage UTF-8).

5.4.4.1.2 Adresses HTTP

Dans cette section, vous pouvez spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification.

Par défaut, les trois listes suivantes sont disponibles :

- **Liste des adresses exclues de la vérification** - Aucune vérification de la présence de code malveillant n'est effectuée pour les adresses répertoriées dans la liste.
- **Liste des adresses autorisées** - Si l'option **N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées** est activée et si la liste des adresses bloquées contient un astérisque (correspond à tout), l'utilisateur n'est autorisé à accéder qu'aux adresses répertoriées dans cette liste. Les adresses de cette liste sont autorisées, même si elles sont incluses dans la liste des adresses bloquées.
- **Liste des adresses bloquées** - L'utilisateur n'est pas autorisé à accéder aux adresses répertoriées dans cette liste, à moins qu'elles ne figurent également dans la liste des adresses autorisées.

Cliquez sur **Ajouter** pour créer une liste. Pour supprimer les listes sélectionnées, cliquez sur **Supprimer**.

5.4.5 Protection antihameçonnage

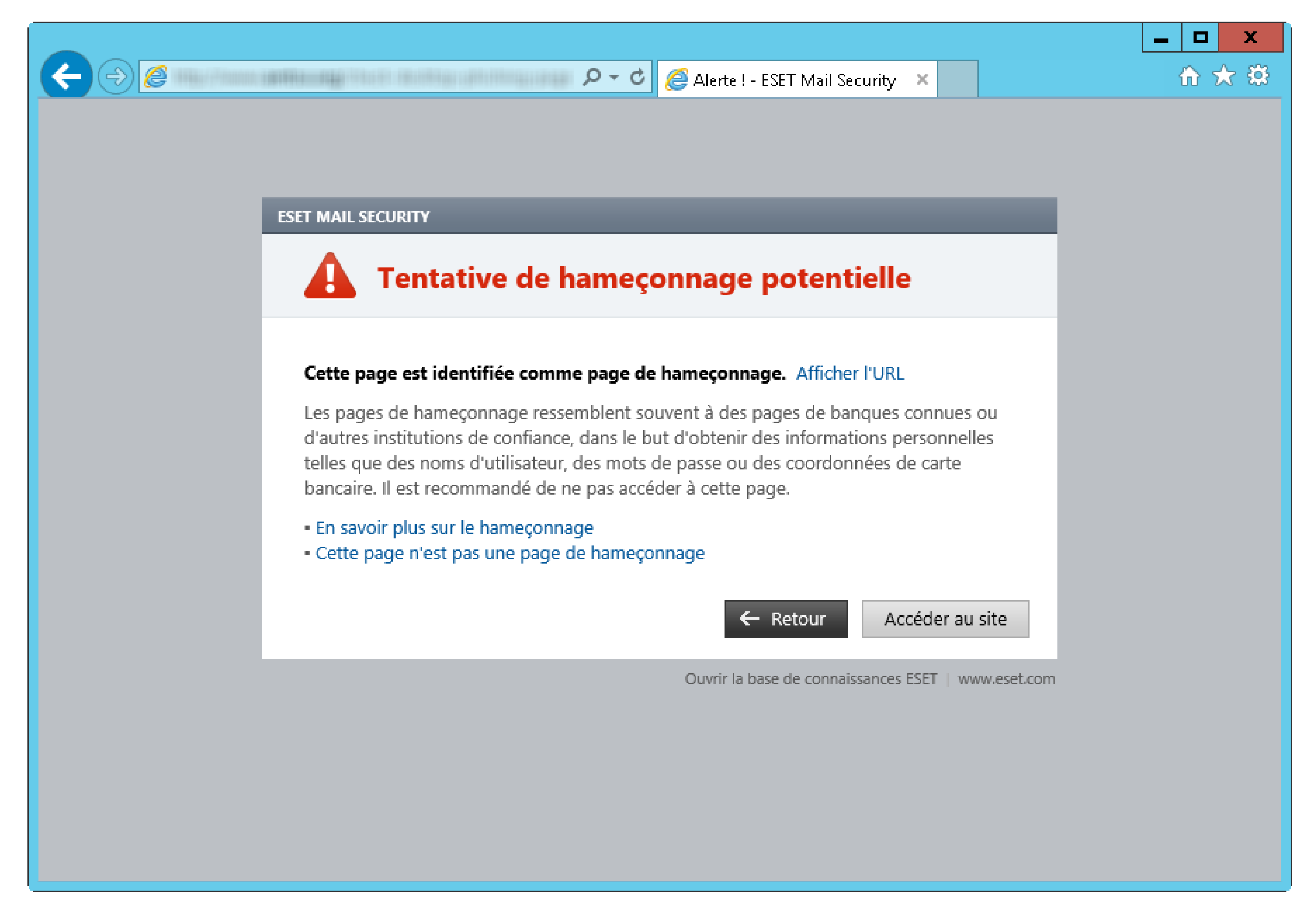
Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse qui consiste à manipuler les utilisateurs pour obtenir des informations confidentielles. L'hameçonnage est souvent utilisé pour accéder à des données sensibles, telles que des numéros de comptes bancaires, des codes secrets, etc. Pour en savoir plus sur cette activité, reportez-vous au glossaire. ESET Mail Security assure une protection antihameçonnage qui permet de bloquer les pages Web connues qui présentent ce type de contenu.

Nous vous recommandons fortement d'activer l'antihameçonnage dans ESET Mail Security. Pour ce faire, accédez à **Configuration avancée** (F5), puis à **Internet et messagerie** > **Protection antihameçonnage**.

Consultez notre article de la base de connaissances pour plus d'informations sur la protection antihameçonnage d'ESET Mail Security.

Accès à un site Web d'hameçonnage

Lorsque vous accédez à un site Web d'hameçonnage reconnu, la boîte de dialogue suivante s'affiche dans votre navigateur Web. Si vous souhaitez toujours accéder au site Web, cliquez sur **Accéder au site** (non recommandé).



REMARQUE : par défaut, les sites Web d'hameçonnage potentiels que vous avez ajoutés à la liste blanche expirent plusieurs heures après. Pour autoriser un site Web de manière permanente, utilisez l'outil Gestion des adresses URL. Dans **Configuration avancée** (F5), développez **Internet et messagerie** > **Protection de l'accès Web** > **Gestion des adresses URL** > **Liste d'adresses**, cliquez sur **Modifier**, puis ajoutez le site Web à modifier à cette liste.

Signalement d'un site de hameçonnage

Le lien Signaler vous permet de signaler un site Web de hameçonnage/malveillant à ESET pour analyse.

REMARQUE : avant de soumettre un site Web à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :

- Le site Web n'est pas du tout détecté.
- Le site Web est détecté à tort comme une menace. Dans ce cas, vous pouvez signaler un site faux positif de hameçonnage.

Vous pouvez également soumettre le site Web par e-mail. Envoyez votre message à l'adresse samples@eset.com. Veillez à utiliser un objet descriptif et indiquez le plus d'informations possible sur le site Web (notez, par exemple, le site Web référant, comment vous avez appris l'existence du site Web, etc.).

5.5 Contrôle de périphérique

ESET Mail Security permet un contrôle automatique des périphériques (CD/DVD/USB). Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de définir les autorisations des utilisateurs à accéder à un périphérique et à l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher l'utilisation de périphériques avec du contenu non sollicité.

Périphériques externes pris en charge :

- Stockage sur disque (disque dur, disque amovible USB)
- CD/DVD
- Imprimante USB
- Stockage FireWire
- Périphérique Bluetooth
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- Port LPT/COM
- Périphérique portable
- Tous les types de périphériques

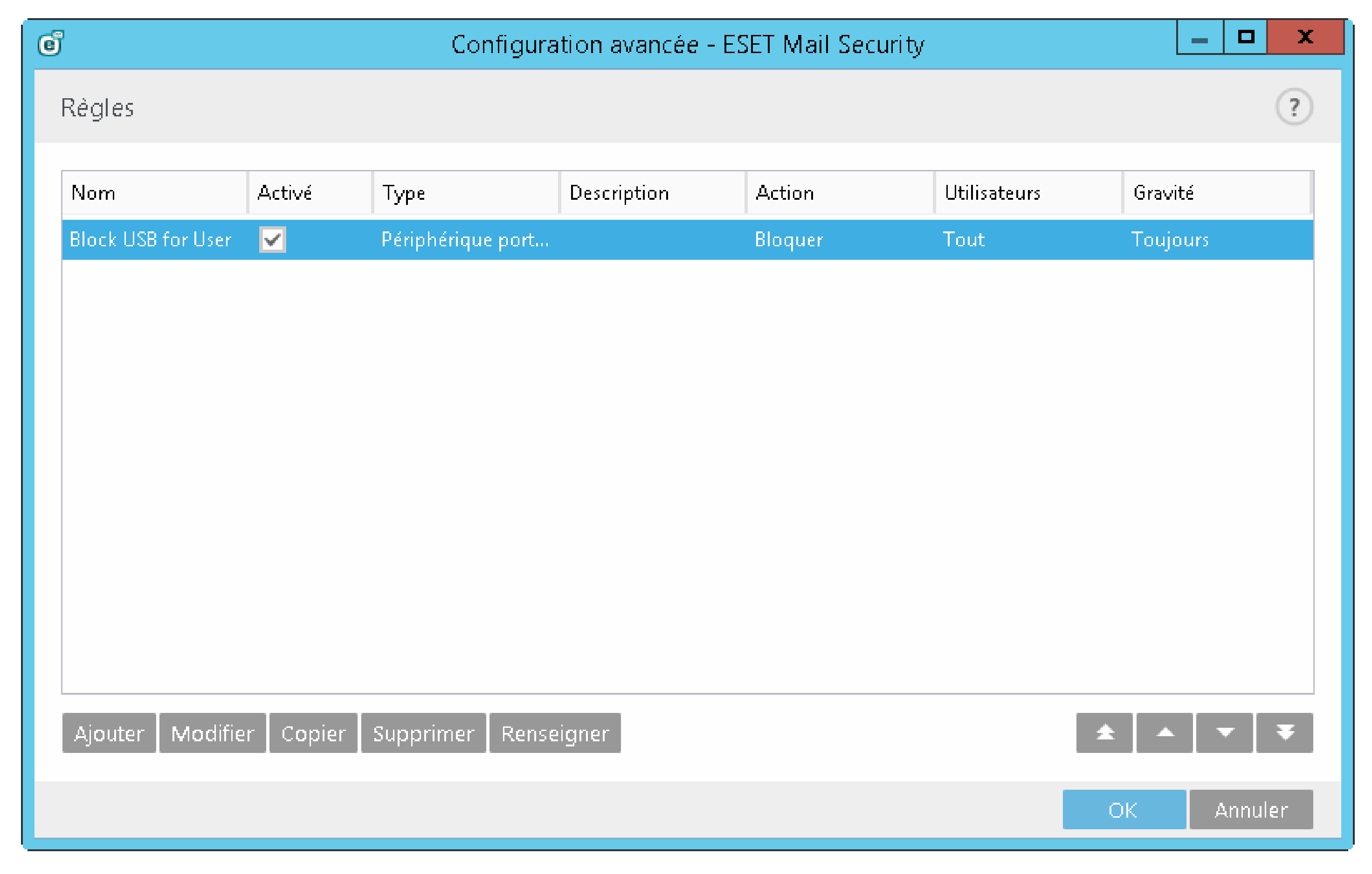
Les options de configuration du contrôle de périphérique peuvent être modifiées dans **Configuration avancée** (F5) > **Contrôle de périphérique**.

Si vous activez l'option **Intégrer au système**, la fonctionnalité de contrôle de périphérique est activée dans ESET Mail Security ; vous devrez redémarrer votre ordinateur pour que cette modification soit prise en compte. Une fois le contrôle de périphérique activé, l'**Éditeur de règles** devient actif et vous permet d'ouvrir la fenêtre Éditeur de règles.

Si un périphérique bloqué par une règle existante est inséré, une fenêtre de notification s'affiche et l'accès au périphérique n'est pas accordé.

5.5.1 Règles du contrôle des périphériques

La fenêtre **Éditeur de règles de contrôle de périphérique** affiche les règles existantes et permet un contrôle précis des périphériques externes que les utilisateurs peuvent connecter à l'ordinateur.



Des périphériques spécifiques peuvent être autorisés ou bloqués par utilisateur, groupe d'utilisateurs ou tout autre paramètre supplémentaire pouvant être spécifié dans la configuration des règles. La liste des règles contient plusieurs descriptions de la règle, telles que son nom, le type de périphérique externe, l'action à exécuter après la connexion d'un périphérique externe à l'ordinateur et le niveau de gravité d'après le journal.

Cliquez sur **Ajouter** ou **Modifier** pour gérer une règle. Cliquez sur **Supprimer** pour supprimer la règle sélectionnée ou désactivez la case à cocher **Activé** en regard d'une règle donnée pour la désactiver. La désactivation d'une règle peut s'avérer utile si vous ne souhaitez pas la supprimer définitivement en vue de la réutiliser ultérieurement.

Copier - Crée une règle à l'aide d'options prédéfinies utilisées pour une autre règle sélectionnée.

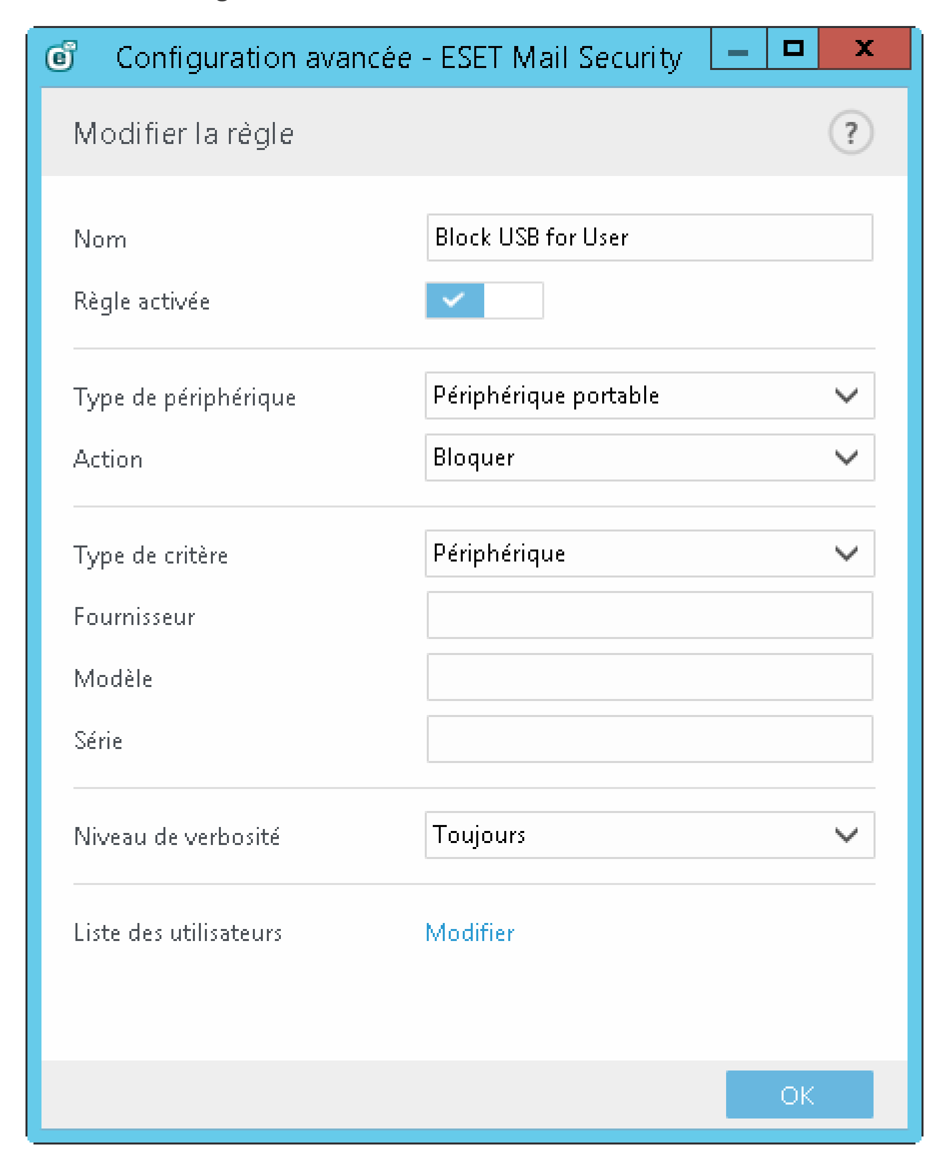
Cliquez sur l'option **Renseigner** pour renseigner automatiquement les paramètres des supports amovibles déjà connectés à votre ordinateur.

Les règles sont classées par ordre de priorité ; les règles de priorité supérieure sont dans la partie supérieure de la liste. Vous pouvez sélectionner plusieurs règles et appliquer des actions, par exemple les supprimer ou les déplacer vers le haut ou le bas de la liste, en cliquant sur **Haut/Monter/Bas/Descendre** (boutons fléchés).

Les entrées de journaux peuvent être affichées dans la fenêtre principale du programme ESET Mail Security dans **Outils** > **Fichiers journaux**.

5.5.2 Ajout de règles de contrôle de périphérique

Une règle de contrôle de périphérique définit l'action qui sera exécutée lorsqu'un périphérique répondant aux critères de la règle est connecté à l'ordinateur.



Entrez une description de la règle dans le champ **Nom** afin de mieux l'identifier. Cliquez sur le bouton bascule situé en regard de l'option **Règle activée** pour désactiver ou activer cette règle ; cette option peut être utile si vous ne souhaitez pas supprimer la règle de façon définitive.

Type de périphérique

Choisissez le type de périphérique externe dans le menu déroulant (Stockage disque/Périphérique portable/ Bluetooth/FireWire...). Les types de périphériques sont hérités du système d'exploitation et sont visibles dans le Gestionnaire de périphériques système si le périphérique est connecté à l'ordinateur. Les périphériques de stockage comprennent les disques externes ou les lecteurs de carte mémoire conventionnels connectés via USB ou FireWire. Les lecteurs de carte à puce regroupent tous les lecteurs de carte avec circuit intégré embarqué, telles que les cartes SIM ou d'authentification. Les scanners ou les appareils photo constituent des exemples de périphériques d'imagerie. Ces périphériques ne fournissent pas d'informations sur les utilisateurs, uniquement sur leurs actions. Cela signifie que les périphériques d'imagerie peuvent être bloqués uniquement de façon globale.

Action

L'accès aux périphériques autres que ceux de stockage peut être autorisé ou bloqué. En revanche, les règles s'appliquant aux périphériques de stockage permettent de sélectionner l'un des paramètres des droits suivants :

- **Lire/Écrire** - L'accès complet au périphérique est autorisé.
- **Bloquer** - L'accès au périphérique est bloqué.

- **Lecture seule** - L'accès en lecture seule au périphérique est autorisé.
- **Avertir** - À chaque connexion d'un périphérique, l'utilisateur est averti s'il est autorisé/bloqué, et une entrée est enregistrée dans le journal. Comme les périphériques ne sont pas mémorisés, une notification s'affiche lors des connexions suivantes d'un même périphérique.

Veuillez noter que tous les droits (actions) ne sont pas disponibles pour tous les périphériques. Si un périphérique comprend un espace de stockage, les quatre actions sont disponibles. Pour les périphériques sans stockage, seules deux options sont disponibles (par exemple, l'action **Lecture seule** n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou bloqué).

Les autres paramètres indiqués ci-dessous peuvent être utilisés pour optimiser les règles et les adapter à des périphériques. Tous les paramètres sont indépendants de la casse :

- **Fabricant** - Permet de filtrer par nom ou ID de fabricant.
- **Modèle** - Nom du périphérique.
- **N° de série** - Les périphériques externes ont généralement leur propre numéro de série. Dans le cas d'un CD/DVD, Il s'agit du numéro de série du support et pas du lecteur.

REMARQUE : si ces trois descripteurs sont vides, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte ne respectent pas la casse et les caractères génériques (*, ?) ne sont pas pris en charge.

Conseil : pour déterminer les paramètres d'un périphérique, créez une règle d'autorisation pour ce type de périphérique, connectez le périphérique à votre ordinateur, puis vérifiez les détails du périphérique dans le journal du contrôle de périphérique.

Gravité

- **Toujours** - Consigne tous les événements.
- **Diagnostic** - Consigne les informations nécessaires au réglage du programme.
- **Informations** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissement** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Aucun** - Aucun journal n'est enregistré.

Les règles peuvent être limitées à certains utilisateurs ou groupes d'utilisateurs en les ajoutant à la **Liste des utilisateurs** :

- **Ajouter** - Ouvre la boîte de dialogue **Types d'objet : utilisateurs ou groupes** qui permet de sélectionner les utilisateurs voulus.
- **Supprimer** - Supprime l'utilisateur sélectionné du filtre.

i **REMARQUE** : tous les périphériques peuvent être filtrés par les règles de l'utilisateur (par exemple, les périphériques d'image ne fournissent pas d'informations sur les utilisateurs, uniquement sur les actions effectuées).

5.5.3 Périphériques détectés

Le bouton **Renseigner** permet de donner une vue d'ensemble de tous les périphériques actuellement connectés avec les informations suivantes : le type de périphérique, le fournisseur, le modèle et le numéro de série (le cas échéant). Si vous sélectionnez un périphérique (dans la liste des périphériques détectés) et cliquez sur **OK**, une fenêtre d'éditeur de règles s'affiche avec des informations prédéfinies (vous pouvez ajuster tous les paramètres).

5.5.4 Groupe de périphériques

 Un périphérique connecté à votre ordinateur peut présenter un risque de sécurité.

La fenêtre Groupes de périphériques se divise en deux parties. La partie droite de la fenêtre contient la liste des périphériques appartenant à un groupe donné. La partie gauche répertorie la liste des groupes existants. Sélectionnez le groupe contenant les périphériques que vous souhaitez afficher dans le volet droit.

Lorsque vous ouvrez la fenêtre Groupes de périphériques et que vous sélectionnez un groupe, vous pouvez ajouter ou supprimer des périphériques de la liste. Une autre méthode pour ajouter des périphériques au groupe consiste à les importer à partir d'un fichier. Vous pouvez aussi cliquer sur le bouton **Renseigner** pour que tous les périphériques connectés à votre ordinateur soient répertoriés dans la fenêtre **Périphériques détectés**. Sélectionnez un périphérique dans la liste renseignée, puis cliquez sur **OK** pour l'ajouter au groupe.

Éléments de commande

Ajouter : vous pouvez ajouter un groupe en saisissant son nom. Vous pouvez également ajouter un périphérique à un groupe existant. Vous pouvez éventuellement indiquer des informations détaillées (le nom du fabricant, le modèle et le numéro de série, par exemple) selon l'endroit de la fenêtre où vous avez cliqué sur le bouton.

Modifier - Permet de modifier le nom du groupe sélectionné ou les paramètres du périphérique inséré (fabricant, modèle, numéro de série, etc.).

Supprimer - Permet de supprimer le groupe ou le périphérique sélectionné selon l'endroit de la fenêtre où vous avez cliqué.

Importer - Permet d'importer la liste de périphériques à partir d'un fichier.

Le bouton **Renseigner** permet de donner une vue d'ensemble de tous les périphériques actuellement connectés avec les informations suivantes : le type de périphérique, le fournisseur, le modèle et le numéro de série (le cas échéant).

Une fois la personnalisation terminée, cliquez sur **OK**. Cliquez sur **Annuler** si vous souhaitez fermer la fenêtre **Groupes de périphériques** sans enregistrer les modifications.

CONSEIL : vous pouvez créer des groupes de périphériques différents auxquels différentes règles sont appliquées. Vous pouvez également créer un seul groupe de périphériques auquel la règle avec l'action **Lire/Écrire** ou **Lecture seule** sont appliquées. Les périphériques non reconnus sont ainsi bloqués par le contrôle de périphérique lorsqu'ils sont connectés à votre ordinateur.

Il convient de noter que toutes les actions (autorisations) ne sont pas disponibles pour tous les types de périphériques. Pour les périphériques de stockage, les quatre actions sont disponibles. Pour les périphériques autres que les périphériques de stockage, seules trois actions sont disponibles (par exemple, l'action **Lecture seule** n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou sujet à un avertissement).

5.6 Outils

La liste suivante répertorie les paramètres avancés de tous les outils proposés par ESET Mail Security dans l'onglet **Outils** de la fenêtre principale de l'interface.

5.6.1 ESET Live Grid

ESET Live Grid est un système avancé d'avertissement anticipé constitué de plusieurs technologies de cloud. Il contribue à la détection des nouvelles menaces en s'appuyant sur l'évaluation de la réputation et améliore les performances d'analyse par la mise en liste blanche. Les informations sur les nouvelles menaces sont envoyées en temps réel dans le cloud, ce qui permet aux laboratoires d'ESET de lutte contre les logiciels malveillants d'assurer en permanence une protection à jour et constante. Les utilisateurs peuvent s'informer de la réputation des processus et des fichiers en cours d'exécution depuis l'interface du programme ou à partir d'un menu contextuel comprenant des informations supplémentaires mises à disposition par ESET Live Grid. Lors de l'installation d'ESET Mail Security, sélectionnez l'une des options suivantes :

1. Vous pouvez décider de ne pas activer ESET Live Grid. Le logiciel ne perd aucune fonctionnalité, mais ESET Mail Security peut répondre dans certains cas plus lentement aux nouvelles menaces que la mise à jour de la base des signatures de virus.
2. Vous pouvez configurer ESET Live Grid afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où a été détecté le code dangereux. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces.

Le système ESET Live Grid collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Par défaut, ESET Mail Security est configuré pour soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Les fichiers ayant une extension définie (*.doc* ou *.xls* par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

Le système de réputation ESET Live Grid permet la mise en liste blanche ou noire dans le cloud. Pour accéder aux paramètres d'ESET Live Grid, appuyez sur F5 pour passer à la configuration avancée, puis développez **Outils** > **ESET Live Grid**.

Activer le système de réputation ESET Live Grid (recommandé) - Le système de réputation ESET Live Grid améliore l'efficacité des solutions de protection contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments mis en liste blanche et noire dans le cloud.

Soumettre des statistiques anonymes - Permet à ESET de collecter des informations sur les nouvelles menaces détectées telles que le nom de la menace, la date et l'heure de détection, la méthode de détection et les métadonnées associées, la version du produit et la configuration (informations sur votre système).

Soumettre les fichiers - Les fichiers suspects ressemblant à des menaces et/ou des fichiers aux caractéristiques ou au comportement inhabituels peuvent être envoyés pour analyse à ESET.

Sélectionnez **Activer la journalisation** pour créer un journal d'événements permettant d'enregistrer les soumissions des fichiers et des informations statistiques. Cette option permettra de consigner les fichiers ou statistiques envoyés dans le journal des événements.

Adresse électronique de contact (facultatif) - Votre adresse électronique peut être incluse avec les fichiers suspects. Nous pourrons l'utiliser pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

Exclusion - Le filtre Exclusion permet d'exclure certains fichiers/dossiers de la soumission (par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul). Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les fichiers les plus courants sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Si vous avez déjà utilisé le système ESET Live Grid et l'avez désactivé, il est possible qu'il reste des paquets de données à envoyer. Même après la désactivation, ces paquets sont envoyés à ESET. Une fois toutes les informations actuelles envoyées, plus aucun paquet ne sera créé.

5.6.1.1 Filtre d'exclusion

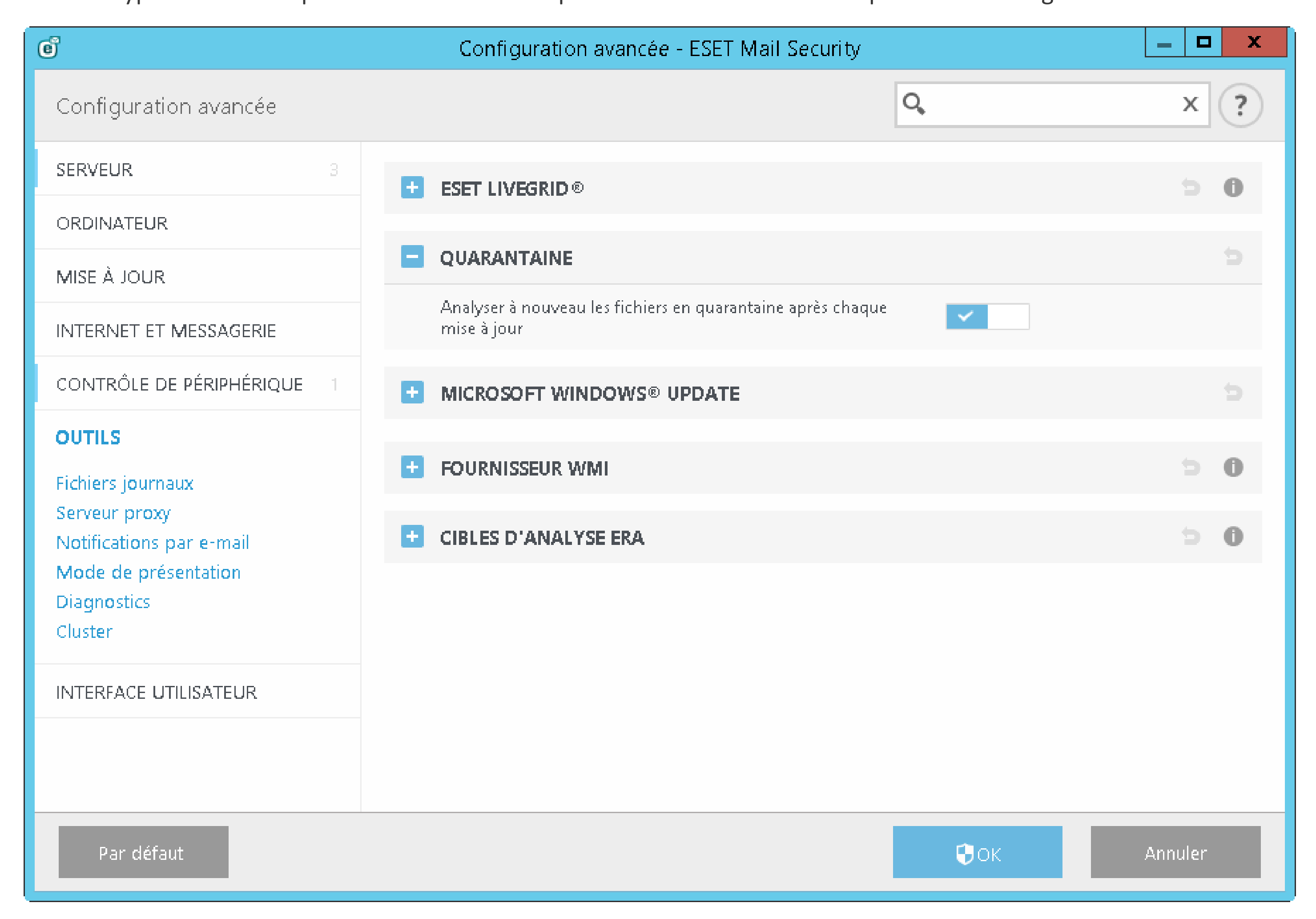
L'option **Modifier** en regard d'Exclusions dans ESET Live Grid permet de configurer le mode de soumission des menaces au laboratoire des virus d'ESET pour analyse.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. S'il s'agit d'une application malveillante, sa détection est ajoutée à la prochaine mise à jour de la base des signatures de virus.

5.6.2 Quarantaine

Les fichiers infectés ou suspects sont stockés sous une forme bénigne dans le dossier de quarantaine. Par défaut, le module de protection en temps réel place en quarantaine les fichiers nouvellement créés afin d'éviter toute infection.

Analyser à nouveau les fichiers en quarantaine après chaque mise à jour - Tous les fichiers en quarantaine sont analysés après chaque mise à jour de la base des signatures de virus. Cette option est particulièrement utile lorsqu'un fichier a été placé en quarantaine après avoir été détecté comme faux positif. Si cette option est activée, certains types de fichiers peuvent être automatiquement restaurés à leur emplacement d'origine.



5.6.3 Microsoft Windows Update

Les mises à jour de Windows apportent des corrections importantes aux vulnérabilités potentiellement dangereuses et améliorent le niveau général de sécurité de votre ordinateur. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET Mail Security vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez. Les niveaux suivants sont disponibles :

- **Pas de mise à jour** - Aucune mise à jour système n'est proposée au téléchargement.
- **Mises à jour optionnelles** - Les mises à jour marquées comme étant faiblement prioritaires et au-dessus sont proposées au téléchargement.
- **Mises à jour recommandées** - Les mises à jour marquées comme étant courantes et au-dessus sont proposées au téléchargement.
- **Mises à jour importantes** - Les mises à jour marquées comme étant importantes et au-dessus sont proposées au téléchargement.
- **Mises à jour critiques** - Seules les mises à jour critiques sont proposées pour le téléchargement.

Cliquez sur **OK** pour enregistrer les modifications. La fenêtre Mises à jour système s'affiche après la vérification de l'état à l'aide du serveur de mise à jour. Les informations de mise à jour système ne sont peut-être pas immédiatement disponibles après l'enregistrement des modifications.

5.6.4 Fournisseur WMI

À propos de WMI

Windows Management Instrumentation (WMI) est la mise en œuvre Microsoft de WBEM (Web-Based Enterprise Management), l'initiative du secteur visant à développer une norme de technologie pour l'accès aux informations de gestion dans les environnements d'entreprise.

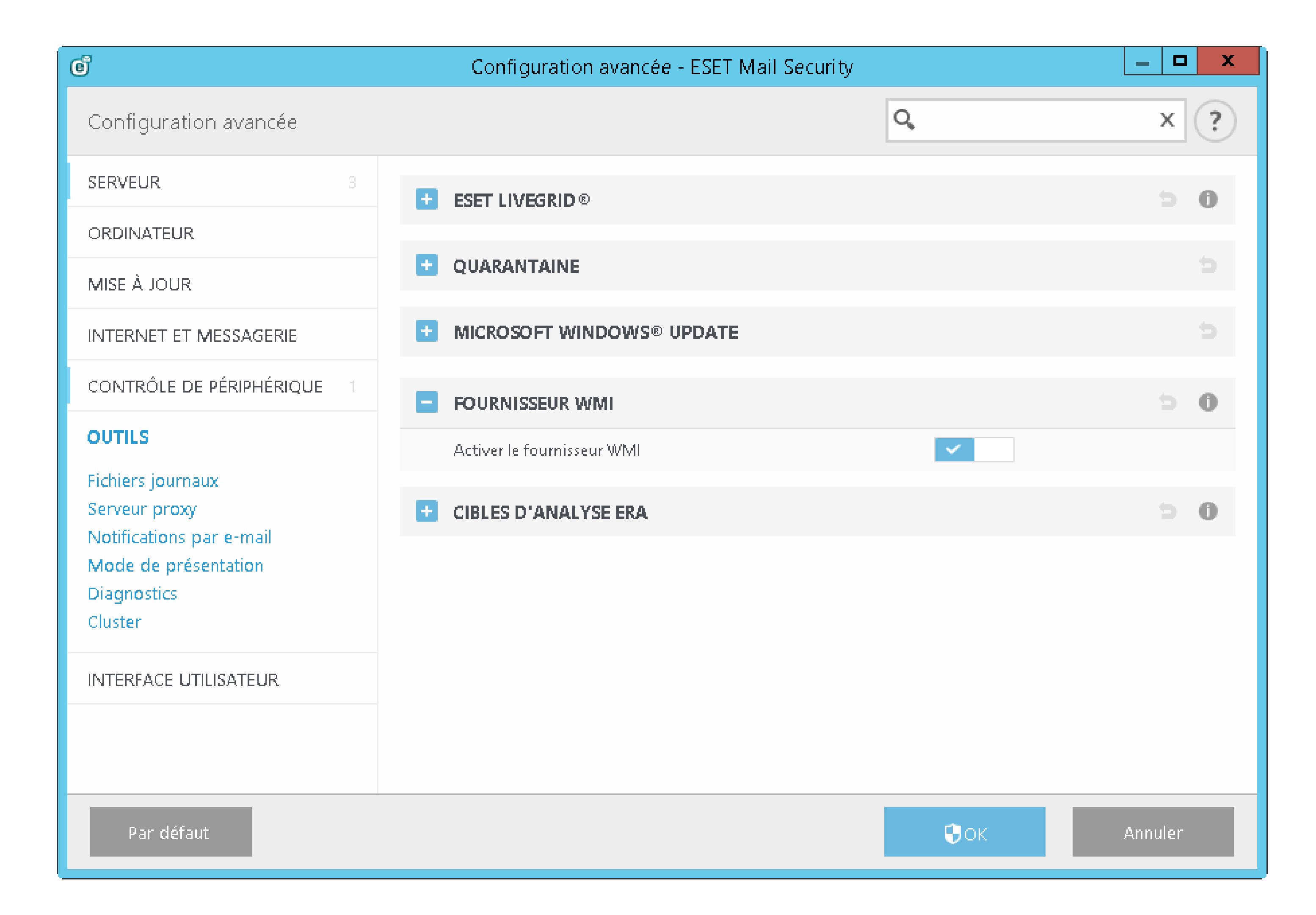
Pour plus d'informations sur WMI, reportez-vous à la page http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

Fournisseur WMI ESET

Le fournisseur WMI d'ESET a pour objectif de permettre la surveillance à distance des produits ESET dans un environnement d'entreprise sans exiger de logiciel ou d'outils ESET. En soumettant le produit de base, l'état et les statistiques par l'intermédiaire de WMI, nous améliorons considérablement la capacité de surveillance des produits ESET par les administrateurs d'entreprise. Les administrateurs peuvent profiter des différentes méthodes d'accès proposées par WMI (ligne de commande, scripts et outils de surveillance d'entreprise tiers) pour surveiller l'état de leurs produits ESET.

La mise en œuvre actuelle fournit un accès en lecture seule aux informations de base sur les produits et les fonctionnalités installées, l'état et les statistiques de protection des différents scanners, ainsi que les fichiers journaux du produit.

Le fournisseur WMI permet d'utiliser les outils et l'infrastructure WMI Windows standard pour lire l'état du produit et les journaux correspondants.



5.6.4.1 Données fournies

Toutes les classes WMI liées au produit ESET se trouvent dans l'espace de noms « root\ESET ». Les classes suivantes, décrites plus en détail ci-dessous, sont actuellement mises en œuvre :

Général :

- ESET_Product
- ESET_Features
- ESET_Statistics

Journaux :

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_GreylistLog
- ESET_SpamLog

Classe ESET_Product

Il ne peut y avoir qu'une seule instance de la classe ESET_Product. Pour connaître les propriétés de cette classe, reportez-vous aux informations générales concernant le produit ESET installé :

- **ID** - Identifiant du type de produit, par exemple « essbe »
- **Name** - Nom du produit, « ESET Security » par exemple
- **Edition** - Édition du produit, « Microsoft SharePoint Server » par exemple
- **Version** - Version du produit, « 4.5.15013.0 » par exemple
- **VirusDBVersion** - Version de la base des virus, « 7868 (20130107) » par exemple
- **VirusDBLastUpdate** - Horodatage de la dernière mise à jour de la base des virus. La chaîne contient l'horodatage au format WMI, par exemple « 20130118115511.000000+060 »
- **LicenseExpiration** - Expiration de la licence. La chaîne contient l'horodatage au format WMI, par exemple « 20130118115511.000000+060 »
- **KernelRunning** - Valeur booléenne indiquant si le service eKrn est en cours d'exécution sur la machine, par exemple « TRUE »
- **StatusCode** - Nombre indiquant l'état de protection du produit : 0 - Vert (OK), 1 - Jaune (avertissement), 2 - Rouge (erreur)
- **StatusText** - Message indiquant la raison d'un code d'état différent de zéro ; dans les autres cas, la valeur est Null

Classe ESET_Features

La classe ESET_Features comporte plusieurs instances en fonction du nombre de fonctionnalités du produit. Chaque instance contient :

- **Name** - Nom de la fonctionnalité (les noms sont répertoriés ci-dessous)
- **Status** - État de la fonctionnalité : 0 - Inactif, 1 - Désactivé, 2 - Activé

La liste des chaînes représente les fonctionnalités du produit actuellement reconnues :

- **CLIENT_FILE_AV** - Protection antivirus en temps réel du système de fichiers
- **CLIENT_WEB_AV** - Protection antivirus Web du client
- **CLIENT_DOC_AV** - Protection antivirus des documents du client
- **CLIENT_NET_FW** - Pare-feu personnel du client
- **CLIENT_EMAIL_AV** - Protection antivirus de la messagerie du client
- **CLIENT_EMAIL_AS** - Protection antispam de la messagerie du client
- **SERVER_FILE_AV** - Protection antivirus en temps réel des fichiers stockés sur le serveur de fichiers protégé, par exemple les fichiers d'une base de données de contenus SharePoint dans le cas d'ESET Mail Security
- **SERVER_EMAIL_AV** - Protection antivirus de la messagerie du serveur protégé, par exemple courriers dans MS Exchange ou dans IBM Lotus Domino
- **SERVER_EMAIL_AS** - Protection antispam de la messagerie du serveur protégé, par exemple courriers dans MS Exchange ou dans IBM Lotus Domino
- **SERVER_GATEWAY_AV** - Protection antivirus des protocoles réseau protégés sur la passerelle
- **SERVER_GATEWAY_AS** - Protection antispam des protocoles réseau protégés sur la passerelle

Classe ESET_Statistics

La classe ESET_Statistics comporte plusieurs instances en fonction du nombre de scanners du produit. Chaque instance contient :

- Scanner - Code chaîne du scanner, par exemple « CLIENT_FILE »
- Total - Nombre total de fichiers analysés
- Infected - Nombre de fichiers infectés détectés
- Cleaned - Nombre de fichiers nettoyés
- Timestamp - Horodatage de la dernière modification des statistiques. Format WMI, par exemple « 20130118115511.000000+060 »
- ResetTime - Horodatage de la dernière réinitialisation des compteurs statistiques. Format WMI, par exemple « 20130118115511.000000+060 »

La liste des chaînes représente les scanners actuellement reconnus :

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Classe ESET_ThreatLog

La classe ESET_ThreatLog comporte plusieurs instances, chacune d'entre elles représentant une entrée du journal Menaces détectées. Chaque instance contient :

- **ID** - Identifiant unique de cette entrée de journal
- **Timestamp** - Horodatage de création de l'entrée de journal (au format WMI)
- **LogLevel** - Gravité de l'entrée de journal, exprimée sous la forme d'un chiffre compris entre 0 et 8. Les valeurs correspondent aux niveaux nommés suivants : Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner** - Nom du scanner qui a créé cet événement de journal.
- **ObjectType** - Type de l'objet qui a produit cet événement de journal.
- **ObjectName** - Nom de l'objet qui a produit cet événement de journal.
- **Threat** - Nom de la menace qui a été détectée dans l'objet décrit par les propriétés ObjectName et ObjectType
- **Action** - Action exécutée après l'identification de la menace
- **User** - Compte utilisateur qui a provoqué la génération de cet événement de journal
- **Information** - Description complémentaire de l'événement

ESET_EventLog

La classe ESET_EventLog comporte plusieurs instances, chacune d'entre elles représentant une entrée du journal Événements. Chaque instance contient :

- **ID** - Identifiant unique de cette entrée de journal
- **Timestamp** - Horodatage de création de l'entrée de journal (au format WMI)
- **LogLevel** - Gravité de l'entrée de journal, exprimée sous la forme d'un chiffre compris entre 0 et 8. Les valeurs correspondent aux niveaux nommés suivants : Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Module** - Nom du module qui a créé cet événement de journal.
- **Event** - Description de l'événement.
- **User** - Compte utilisateur qui a provoqué la génération de cet événement de journal.

ESET_ODFileScanLogs

La classe ESET_ODFileScanLogs comporte plusieurs instances, chacune d'entre elles représentant une entrée d'analyse de fichier à la demande. Elle équivaut à la liste de journaux Analyse de l'ordinateur à la demande de l'interface utilisateur graphique. Chaque instance contient :

- **ID** - Identifiant unique de ce journal à la demande.
- **Timestamp** - Horodatage de création du journal (au format WMI).
- **Targets** - Dossiers/Objets cibles de l'analyse
- **TotalScanned** - Nombre total d'objets analysés
- **Infected** - Nombre d'objets infectés détectés
- **Cleaned** - Nombre d'objets nettoyés
- **Status** - État de l'analyse

ESET_ODFileScanLogRecords

La classe ESET_ODFileScanLogRecords comporte plusieurs instances, chacune d'entre elles représentant une entrée de l'un des journaux d'analyse représentés par les instances de la classe ESET_ODFileScanLogs. Les instances de cette classe fournissent les entrées de journal de toutes les analyses à la demande/tous les journaux. Lorsqu'une seule instance de journal d'analyse est requise, les instances doivent être filtrées par la propriété LogID. Chaque instance de classe contient :

- **LogID** - Identifiant du journal d'analyse auquel appartient cette entrée (identifiant de l'une des instances de la classe ESET_ODFileScanLogs)
- **ID** - Identifiant unique de cette entrée de journal d'analyse
- **Timestamp** - Horodatage de création de l'entrée de journal (au format WMI)
- **LogLevel** - Gravité de l'entrée de journal, exprimée sous la forme d'un chiffre compris entre 0 et 8. Les valeurs correspondent aux niveaux nommés suivants : Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - Message proprement dit du journal

ESET_ODServerScanLogs

La classe ESET_ODServerScanLogs comporte plusieurs instances, chacune d'entre elles représentant une exécution de l'analyse de serveur à la demande. Chaque instance contient :

- **ID** - Identifiant unique de ce journal à la demande.
- **Timestamp** - Horodatage de création du journal (au format WMI).
- **Targets** - Dossiers/Objets cibles de l'analyse
- **TotalScanned** - Nombre total d'objets analysés
- **Infected** - Nombre d'objets infectés détectés
- **Cleaned** - Nombre d'objets nettoyés
- **RuleHits** - Nombre total d'applications des règles
- **Status** - État de l'analyse

ESET_ODServerScanLogRecords

La classe ESET_ODServerScanLogRecords comporte plusieurs instances, chacune d'entre elles représentant une entrée de l'un des journaux d'analyse représentés par les instances de la classe ESET_ODServerScanLogs. Les instances de cette classe fournissent les entrées de journal de toutes les analyses à la demande/tous les journaux. Lorsqu'une seule instance de journal d'analyse est requise, les instances doivent être filtrées par la propriété LogID. Chaque instance de classe contient :

- **LogID** - Identifiant du journal d'analyse auquel appartient cette entrée (identifiant de l'une des instances de la classe ESET_ ODServerScanLogs)
- **ID** - Identifiant unique de cette entrée de journal d'analyse
- **Timestamp** - Horodatage de création de l'entrée de journal (au format WMI)
- **LogLevel** - Gravité de l'entrée de journal, exprimée sous la forme d'un chiffre compris entre 0 et 8. Les valeurs correspondent aux niveaux nommés suivants : Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - Message proprement dit du journal

ESET_GreylistLog

La classe ESET_GreylistLog comporte plusieurs instances, chacune d'entre elles représentant une entrée du journal Liste grise. Chaque instance contient :

- **ID** - Identifiant unique de cette entrée de journal
- **Timestamp** - Horodatage de création de l'entrée de journal (au format WMI)
- **LogLevel** - Gravité de l'entrée de journal, exprimée sous la forme d'un chiffre compris entre 0 et 8. Les valeurs correspondent aux niveaux nommés suivants : Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain** - Nom du domaine HELO
- **IP** - Adresse IP de la source
- **Sender** - Expéditeur du courrier électronique
- **Recipient** - Destinataire du courrier électronique
- **Action** - Action effectuée
- **TimeToAccept** - Nombre de minutes après lesquelles le courrier électronique est accepté

ESET_SpamLog

La classe ESET_SpamLog comporte plusieurs instances, chacune d'entre elles représentant une entrée du journal Spamlog. Chaque instance contient :

- **ID** - Identifiant unique de cette entrée de journal
- **Timestamp** - Horodatage de création de l'entrée de journal (au format WMI)
- **LogLevel** - Gravité de l'entrée de journal, exprimée sous la forme d'un chiffre compris entre 0 et 8. Les valeurs correspondent aux niveaux nommés suivants : Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Sender** - Expéditeur du courrier électronique
- **Recipients** - Destinataires du courrier électronique
- **Subject** - Objet du courrier électronique
- **Received** - Heure de la réception
- **Score** - Score de courrier indésirable exprimé en pourcentage [0-100]
- **Reason** - Raison pour laquelle ce courrier électronique a été marqué comme spam
- **Action** - Action effectuée
- **DiagInfo** - Autres informations de diagnostic

5.6.4.2 Accès aux données fournies

Voici quelques exemples indiquant comment accéder aux données WMI ESET depuis la ligne de commande Windows et PowerShell. Ces méthodes devraient fonctionner sur n'importe quel système d'exploitation Windows actuel. Il existe néanmoins de nombreuses autres manières d'accéder aux données depuis d'autres outils et langages de script.

Ligne de commande sans script

L'outil de ligne de commande `wmic` peut être utilisé pour accéder à différentes classes VMI prédéfinies ou personnalisées.

Pour afficher les informations complètes sur le produit sur la machine locale :

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Pour afficher uniquement la version du produit sur la machine locale :

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Pour afficher les informations complètes sur le produit sur une machine distante dont l'adresse IP est IP 10.1.118.180 :

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Pour obtenir et afficher les informations complètes sur le produit sur la machine locale :

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Pour obtenir et afficher les informations complètes sur le produit sur une machine distante dont l'adresse IP est IP 10.1.118.180 :

```
$cred = Get-Credential            # invite l'utilisateur à fournir des informations d'identification et les
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

5.6.5 Cibles à analyser ERA

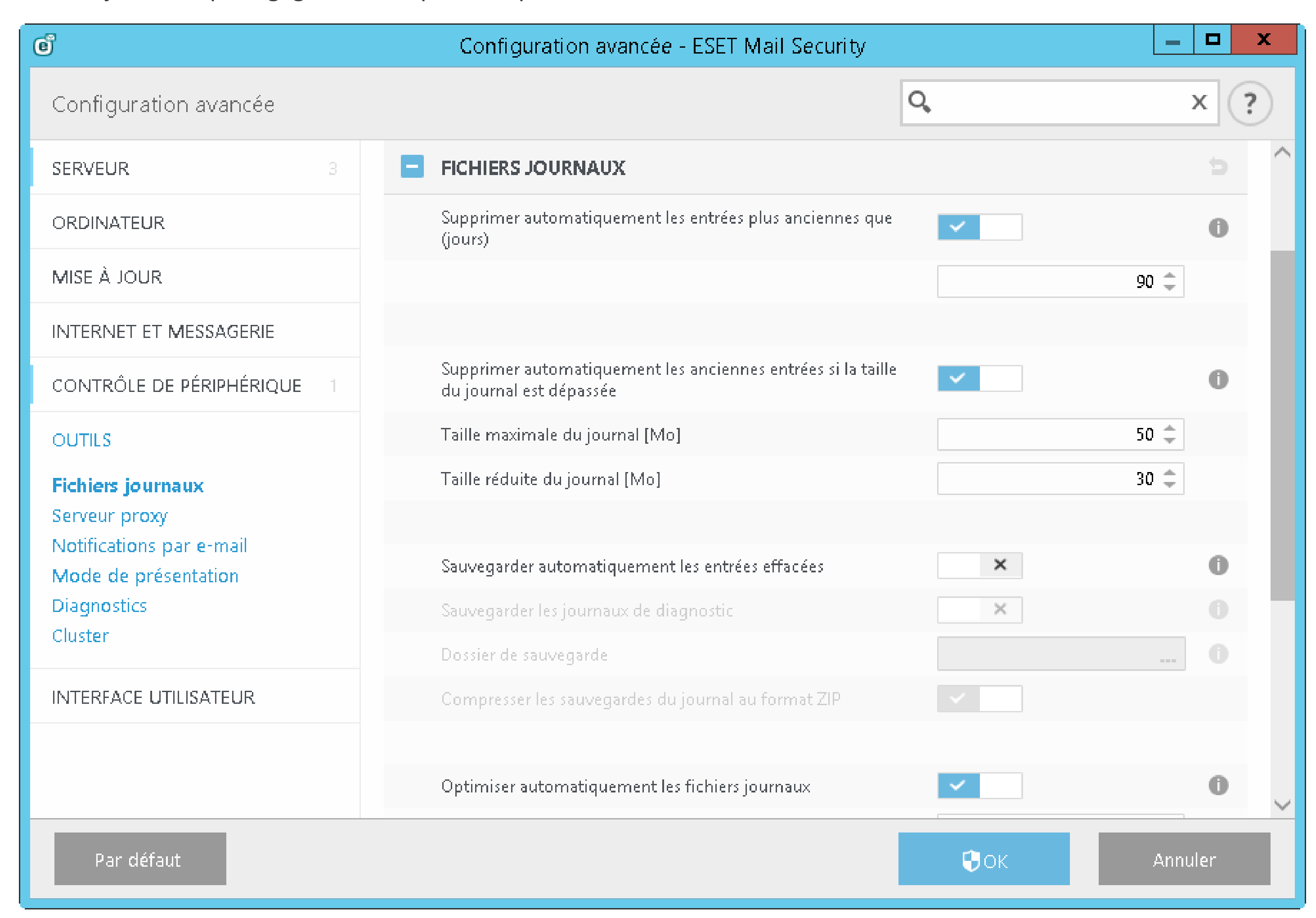
Cette fonctionnalité permet à ESET Remote Administrator d'utiliser des cibles à analyser de base de données à la demande en exécutant la tâche de client **Analyse du serveur** sur un serveur à l'aide de ESET Mail Security.

Lorsque vous activez la fonctionnalité **Générer la liste des cibles**, ESET Mail Security crée une liste de cibles à analyser de base de données actuellement disponibles. Cette liste est régulièrement générée, en fonction de la **Période de mise à jour** définie, exprimée en minutes. Lorsqu'ERA souhaite exécuter une tâche de client **Analyse du serveur**, il collecte la liste et vous permet de sélectionner des cibles à analyser afin d'effectuer une analyse de base de données à la demande sur ce serveur particulier.

5.6.6 Fichiers journaux

La configuration de la consignation d'ESET Mail Security est accessible à partir de la fenêtre principale du programme.

Cliquez sur **Configuration** > **Configuration avancée** > **Outils** > **Fichiers journaux**. La section des fichiers journaux permet de définir la manière dont les journaux sont gérés. Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque.



5.6.6.1 Filtrage des journaux

Les journaux stockent des informations relatives aux événements importants du système. La fonction de filtrage des journaux permet d'afficher les enregistrements propres à un événement en particulier.

Saisissez le mot-clé de recherche dans le champ **Rechercher le texte**. Utilisez le menu déroulant **Rechercher dans les colonnes** pour affiner la recherche.

Types d'enregistrements - Choisissez un ou plusieurs types de journal dans le menu déroulant :

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** - Enregistre les erreurs du type « Erreur de téléchargement du fichier » et les erreurs critiques.
- **Critique** - Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus).

Période - Définissez la période pour laquelle vous souhaitez afficher les résultats.

Mot entier - Cochez cette case si vous souhaitez rechercher des mots complets afin d'obtenir des résultats plus précis.

Respecter la casse - Activez cette option s'il est important d'utiliser des majuscules et des minuscules lors du filtrage.

5.6.6.2 Rechercher dans le journal

Outre le filtrage des journaux, vous pouvez utiliser la fonctionnalité de recherche dans les fichiers journaux. Toutefois, vous pouvez également l'utiliser indépendamment du filtrage des journaux. Ce procédé est utile lorsque vous recherchez des enregistrements précis dans les journaux. Tout comme le filtrage des journaux, cette fonctionnalité de recherche permet de trouver les informations que vous recherchez, notamment lorsque les enregistrements sont très nombreux.

Lorsque vous utilisez la fonction de recherche dans le journal, vous pouvez **rechercher du texte en saisissant une chaîne spécifique**, utiliser le **menu déroulant Rechercher dans les colonnes**, sélectionner **Types d'enregistrements** et définir une **période** afin de ne rechercher que les entrées correspondant à une période définie. En indiquant certaines options de recherche, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre Fichiers journaux.

Rechercher le texte - Saisissez une chaîne (mot ou partie de mot). Seuls les enregistrements contenant cette chaîne sont trouvés. Les autres enregistrements sont omis.

Rechercher dans les colonnes - Sélectionnez les colonnes à prendre en compte lors de la recherche. Vous pouvez cocher une ou plusieurs colonnes à utiliser pour la recherche. Par défaut, toutes les colonnes sont sélectionnées :

- **Heure**
- **Dossier analysé**
- **Événement**
- **utilisateur**

Types d'enregistrements : Choisissez un ou plusieurs types de journal dans le menu déroulant :

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** - Enregistre les erreurs du type « Erreur de téléchargement du fichier » et les erreurs critiques.
- **Critique** - Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus).

Période - Définissez la période pour laquelle vous souhaitez afficher les résultats.

- **Non spécifié** (option par défaut) - N'effectue aucune recherche dans la période ; effectue une recherche dans l'intégralité du journal.
- **Jour antérieur**
- **Dernière semaine**
- **Dernier mois**
- **Période** - Vous pouvez indiquer la période exacte (date et heure) afin de ne rechercher que les enregistrements correspondant à la période indiquée.

Mot entier : recherche uniquement les enregistrements qui correspondent à la chaîne sous forme de mot entier indiquée dans la zone de **recherche**.

Respecter la casse : recherche uniquement les enregistrements qui correspondent à l'utilisation des majuscules et des minuscules indiquée dans la zone de **recherche**.

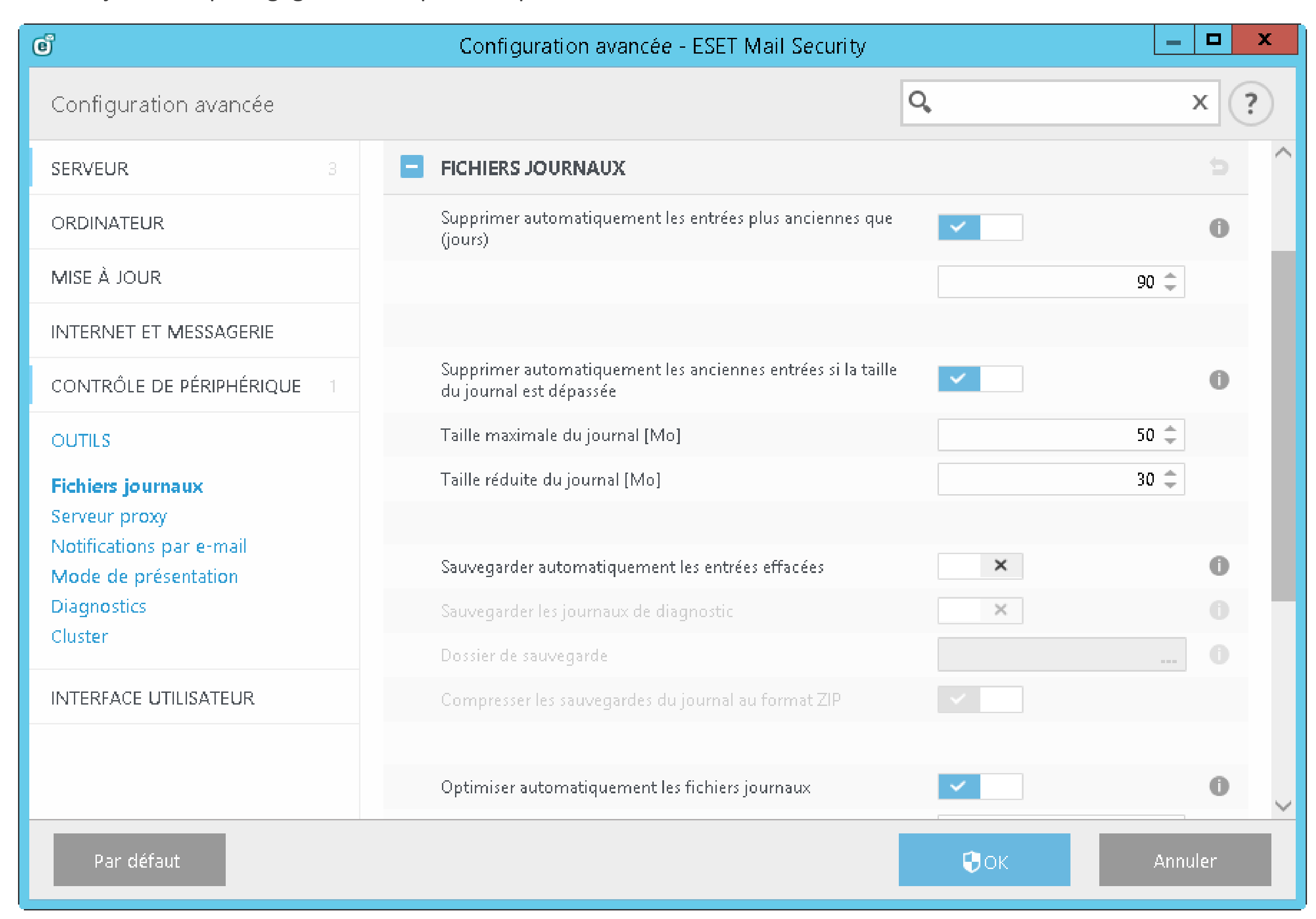
Vers le haut - lance la recherche vers le haut.

Après avoir configuré les options de recherche, cliquez sur **Rechercher** pour lancer la recherche. La recherche s'arrête au premier enregistrement correspondant. Cliquez sur **Rechercher** une nouvelle fois pour afficher les autres enregistrements. La recherche dans les fichiers journaux s'effectue de haut en bas, à partir de la position actuelle (de l'enregistrement sélectionné).

5.6.6.3 Maintenance des journaux

La configuration de la consignation d'ESET Mail Security est accessible à partir de la fenêtre principale du programme.

Cliquez sur **Configuration** > **Configuration avancée** > **Outils** > **Fichiers journaux**. La section des fichiers journaux permet de définir la manière dont les journaux sont gérés. Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque.



- **Supprimer automatiquement les entrées** : les entrées journaux plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.

- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation automatique des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.

- **Verbosité minimale des journaux** : indique la verbosité minimale des journaux. Les options disponibles sont les suivantes :
  - **Entrées diagnostiques** - Consigne toutes les informations nécessaires pour un réglage détaillé du programme et de toutes les entrées ci-dessus.
  - **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
  - **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
  - **Erreurs** - Les erreurs de type « Erreur de téléchargement de fichier » et les erreurs critiques sont enregistrées.
  - **Avertissements critiques** - Répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, etc.).

5.6.7 Serveur proxy

Dans les grands réseaux locaux, la connexion de votre ordinateur à Internet peut s'effectuer par l'intermédiaire d'un serveur proxy. Si c'est le cas, les paramètres suivants doivent être définis. Dans le cas contraire, le programme ne pourra pas se mettre à jour automatiquement. Dans ESET Mail Security, il est possible de configurer le serveur proxy à partir de deux sections de la configuration avancée complète.

Tout d'abord, les paramètres de serveur proxy peuvent être configurés dans **Configuration avancée**, depuis **Outils** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET Mail Security. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, activez l'option **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy**, ainsi que le numéro de **port** de celui-ci.

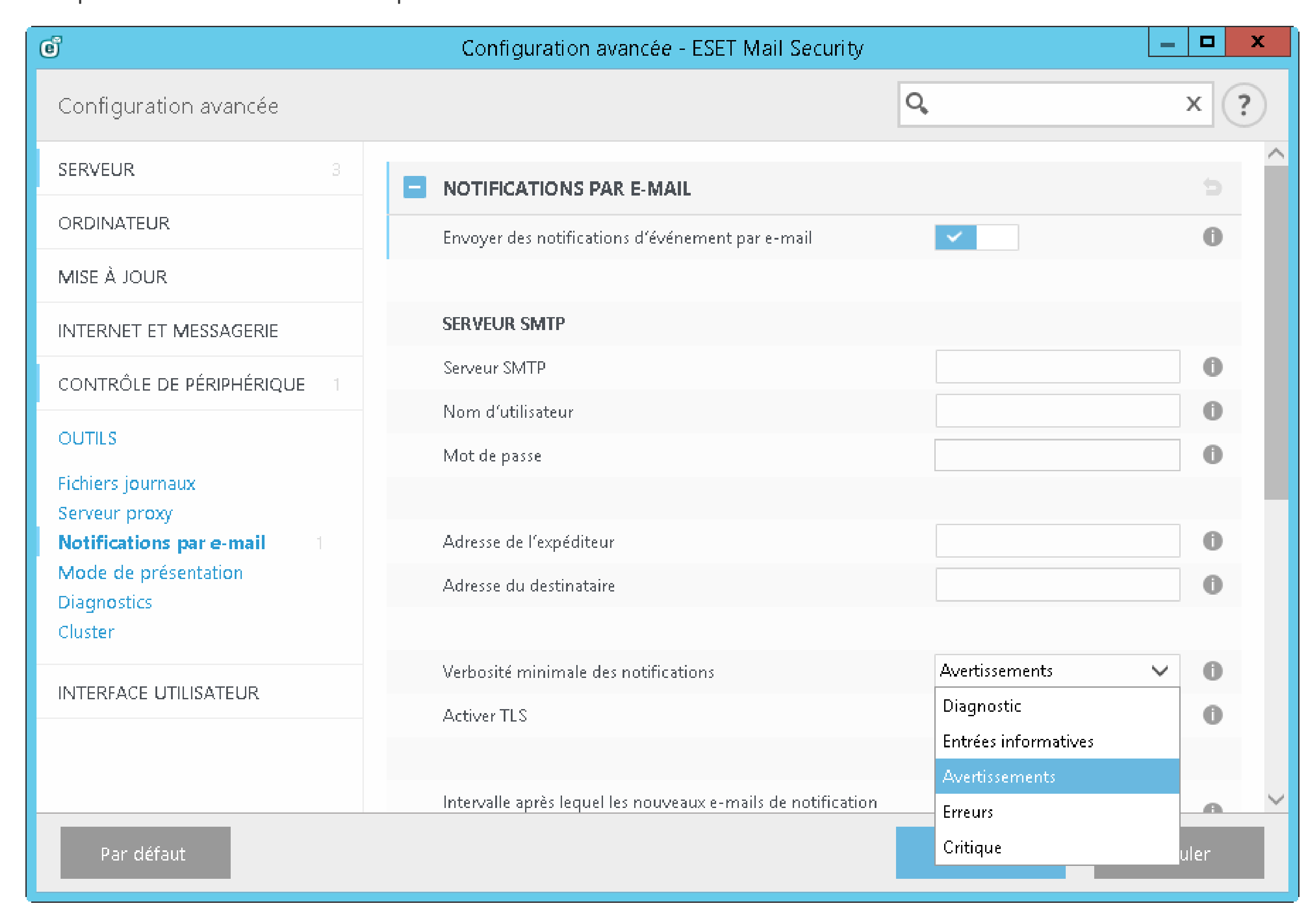
Si la communication avec le serveur proxy exige une authentification, activez l'option **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur **Détecter** pour détecter et renseigner automatiquement les paramètres du serveur proxy. Les paramètres indiqués dans Internet Explorer sont copiés.

i **REMARQUE :** cette fonctionnalité ne récupère pas les données d'authentification (nom d'utilisateur et mot de passe) ; vous devez donc les fournir.

Les paramètres de serveur proxy peuvent également être définis dans la configuration avancée des mises à jour (**Configuration avancée** > **Mise à jour** > **Proxy HTTP** en sélectionnant **Connexion via un serveur proxy** dans le menu déroulant **Mode proxy**). Ce paramètre s'applique au profil de mise à jour donné et est recommandé pour les ordinateurs portables, car il permet de recevoir les mises à jour de la base des signatures de virus depuis différents emplacements. Pour plus d'informations sur ce paramètre, consultez la section Configuration avancée des mises à jour.

5.6.8 Notifications par e-mail

ESET Mail Security peut automatiquement envoyer des courriers électroniques de notification si un événement avec le niveau de verbosité sélectionné se produit. Activez l'option **Envoyer des notifications d'événement par e-mail** pour activer les notifications par e-mail.



REMARQUE : les serveurs SMTP avec chiffrement TLS sont pris en charge par ESET Mail Security.

- **Serveur SMTP -** Le serveur SMTP utilisé pour l'envoi de notifications.
- **Nom d'utilisateur et mot de passe** - Si le serveur SMTP exige une authentification, ces champs doivent être remplis avec un nom d'utilisateur et un mot de passe valides donnant accès au serveur SMTP.

- **Adresse de l'expéditeur** - Ce champ spécifie l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.
- **Adresse du destinataire** - Ce champ spécifie l'adresse du destinataire qui apparaît dans l'en-tête des notifications.

- **Verbosité minimale des notifications** - Spécifie le niveau minimum de verbosité des notifications à envoyer.
- **Activer TLS** - Permet d'activer les messages d'alerte et de notification pris en charge par le chiffrement TLS.

- **Intervalle après lequel les nouveaux e-mails de notification seront envoyés (min)** - Intervalle en minutes après lequel de nouvelles notifications seront envoyées par e-mail. Définissez cette valeur sur 0 si vous souhaitez envoyer ces notifications immédiatement.
- **Envoyer chaque notification dans un e-mail séparé** - Lorsque cette option est activée, le destinataire recevra un nouvel e-mail pour chaque notification spécifique. Cela peut se traduire par la réception d'un nombre important d'e-mails dans une courte période de temps.

Format des messages

- **Format des messages d'événement** - Format des messages d'événement qui s'affichent sur les ordinateurs distants. Voir aussi Modifier le format.
- **Format des messages d'avertissement de menace** - Messages d'alerte et de notification de menace dont le format par défaut est prédéfini. Il est déconseillé de modifier ce format. Toutefois, dans certaines circonstances (par

exemple, si vous avez un système automatisé de traitement des messages), vous serez peut-être amené à modifier le format des messages. Voir aussi Modifier le format.

- **Utiliser les caractères alphabétiques locaux** - Convertit le message électronique au codage ANSI sur la base des paramètres régionaux de Windows (par exemple, windows-1250). Si vous ne sélectionnez pas cette option, le message est converti et codé au format ACSII 7 bits (ainsi, « á » est remplacé par « a » et un symbole inconnu par un « ? »).
- **Utiliser l'encodage des caractères locaux** - Le message électronique source est codé au format Quoted-printable (QP) qui utilise les caractères ASCII et peut correctement transmettre les caractères spéciaux par e-mail au format 8 bits (áéíóú).

5.6.8.1 Format des messages

Les communications entre le programme et l'utilisateur ou l'administrateur système distants se font via la messagerie ou le réseau local (au moyen du service de messagerie Windows®). Le format par défaut des messages d'alerte et des notifications est optimal dans la plupart des situations. Dans certaines situations, le format des messages d'événement doit être changé.

Les mots-clés (chaînes entourées de signes %) sont remplacés dans le message par les informations réelles spécifiées. Les mots-clés suivants sont disponibles :

- **%TimeStamp%** - Date et heure de l'événement
- **%Scanner%** - Module concerné
- **%ComputerName%** - Nom de l'ordinateur sur lequel l'alerte s'est produite
- **%ProgramName%** - Programme ayant généré l'alerte
- **%InfectedObject%** - Nom du fichier, message infecté, etc.
- **%VirusName%** - Identification de l'infection
- **%ErrorDescription%** - Description d'un événement autre qu'un virus

Les mots-clés **%InfectedObject%** et **%VirusName%** ne sont utilisés que dans les messages d'alerte de menace, tandis que le mot-clé **%ErrorDescription%** n'est utilisé que dans les messages d'événement.

5.6.9 Mode de présentation

Le mode de présentation est une fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Il peut également être utilisé au cours de présentations qui ne peuvent pas être interrompues par l'activité antivirus. Lorsqu'il est activé, toutes les fenêtres contextuelles sont désactivées et les tâches planifiées ne sont pas exécutées. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Cliquez sur **Configuration** > **Ordinateur**, puis sur le bouton bascule en regard de l'option **Mode de présentation** pour activer manuellement le mode de présentation. Dans **Configuration avancée** (F5), cliquez sur **Outils** > **Mode de présentation**, puis sur le bouton bascule en regard de l'option **Activer le mode de présentation automatiquement lors de l'exécution d'applications en mode plein écran** pour qu'ESET Mail Security active automatiquement le mode de présentation lorsque les applications sont exécutées en mode plein écran. L'activation du mode de présentation constitue un risque potentiel pour la sécurité. C'est la raison pour laquelle l'icône d'état de la protection située dans la barre des tâches devient orange et affiche un symbole d'avertissement. Ce symbole apparaît également dans la fenêtre principale du programme, où **Mode de présentation activé** apparaît en orange.

Lorsque l'option **Activer le mode de présentation automatiquement lors de l'exécution d'applications en mode plein écran** est activée, le mode de présentation démarre lorsque vous lancez une application en mode plein écran et s'arrête automatiquement lorsque vous quittez l'application. Cette option est particulièrement utile, car elle permet de démarrer le mode de présentation immédiatement après le démarrage d'un jeu, l'ouverture d'une application en mode plein écran ou le démarrage d'une présentation.

Vous pouvez également sélectionner **Désactiver automatiquement le mode de présentation après** pour définir une durée en minutes après laquelle le mode de présentation est automatiquement désactivé.

5.6.10 Diagnostics

Le diagnostic fournit un fichier d'image mémoire en cas de défaillance d'une application lors des processus ESET (par exemple *ekrn*). Dès qu'une application présente une défaillance, un fichier d'image mémoire est généré. Ce fichier permet aux développeurs de déboguer et de résoudre différents problèmes ESET Mail Security. Cliquez sur le menu déroulant en regard de l'option **Type de fichier d'image mémoire**, puis sélectionnez l'une des trois options disponibles :

- Sélectionnez **Désactiver** (valeur par défaut) pour désactiver cette fonctionnalité.
- **Mini** - Enregistre le plus petit ensemble d'informations utiles qui peut permettre d'identifier les raisons de l'arrêt inopiné de l'application. Ce type de fichier d'image mémoire peut être utile lorsque l'espace disponible est limité. Toutefois, en raison des informations limitées qui figurent dans ce fichier, les erreurs qui n'étaient pas directement provoquées par la menace (car cette dernière ne s'exécutait pas au moment du problème) risquent de ne pas être détectées par l'analyse de ce fichier.
- **Complet** - Enregistre tout le contenu de la mémoire système en cas d'arrêt inopiné de l'application. Un fichier d'image mémoire complet peut contenir des données provenant des processus en cours au moment de sa collecte.

Répertoire cible - Répertoire dans lequel est généré le fichier d'image mémoire lors de la défaillance.

Ouvrir le dossier de diagnostics - Cliquez sur **Ouvrir** pour ouvrir ce répertoire dans une nouvelle fenêtre de l'*Explorateur Windows*.

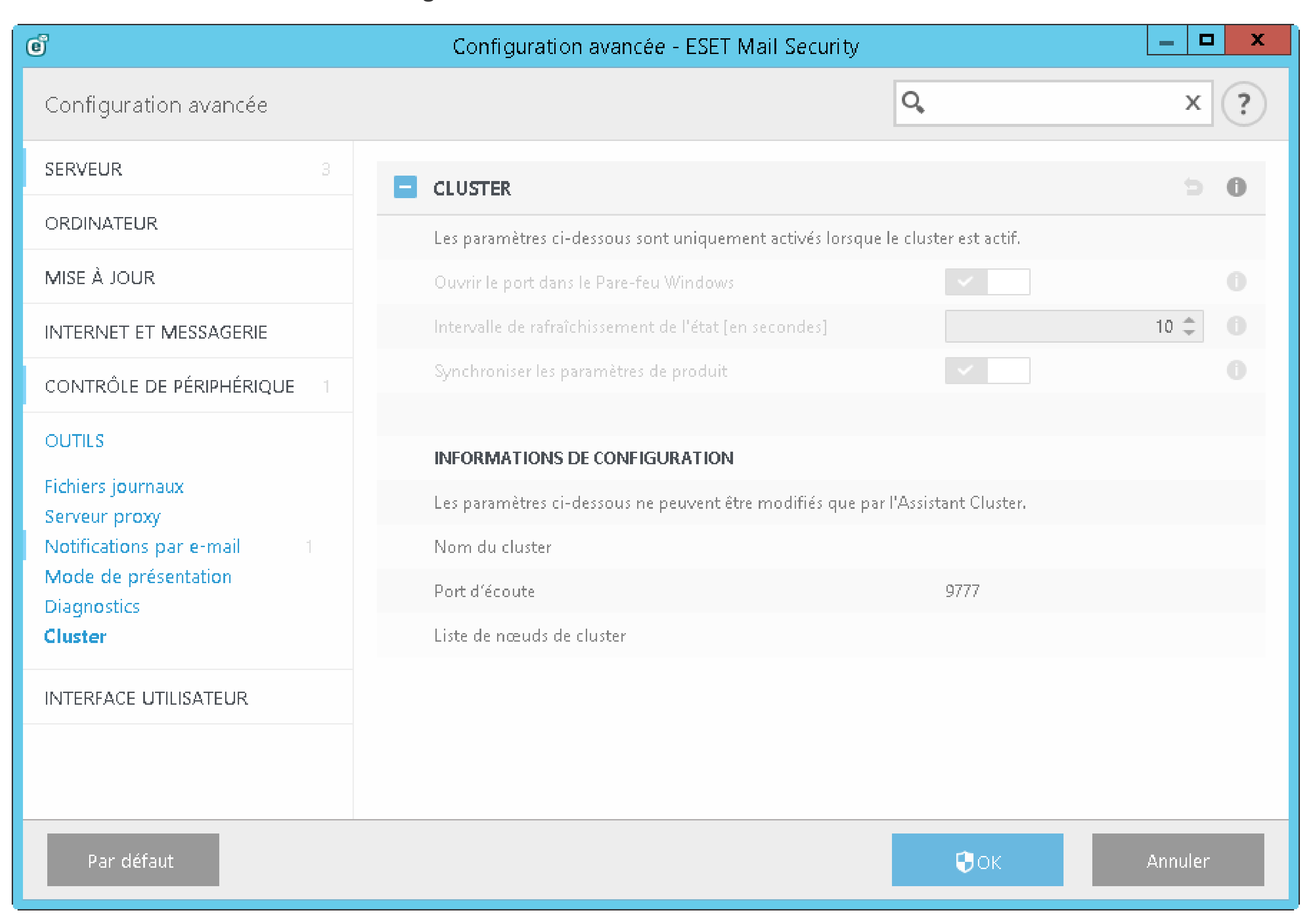
5.6.11 Service client

Soumettre les données de configuration système : dans le menu déroulant, sélectionnez **Toujours soumettre**. Vous pouvez également sélectionner **Demander avant soumission** pour que le système vous demande si vous souhaitez soumettre effectivement les données.

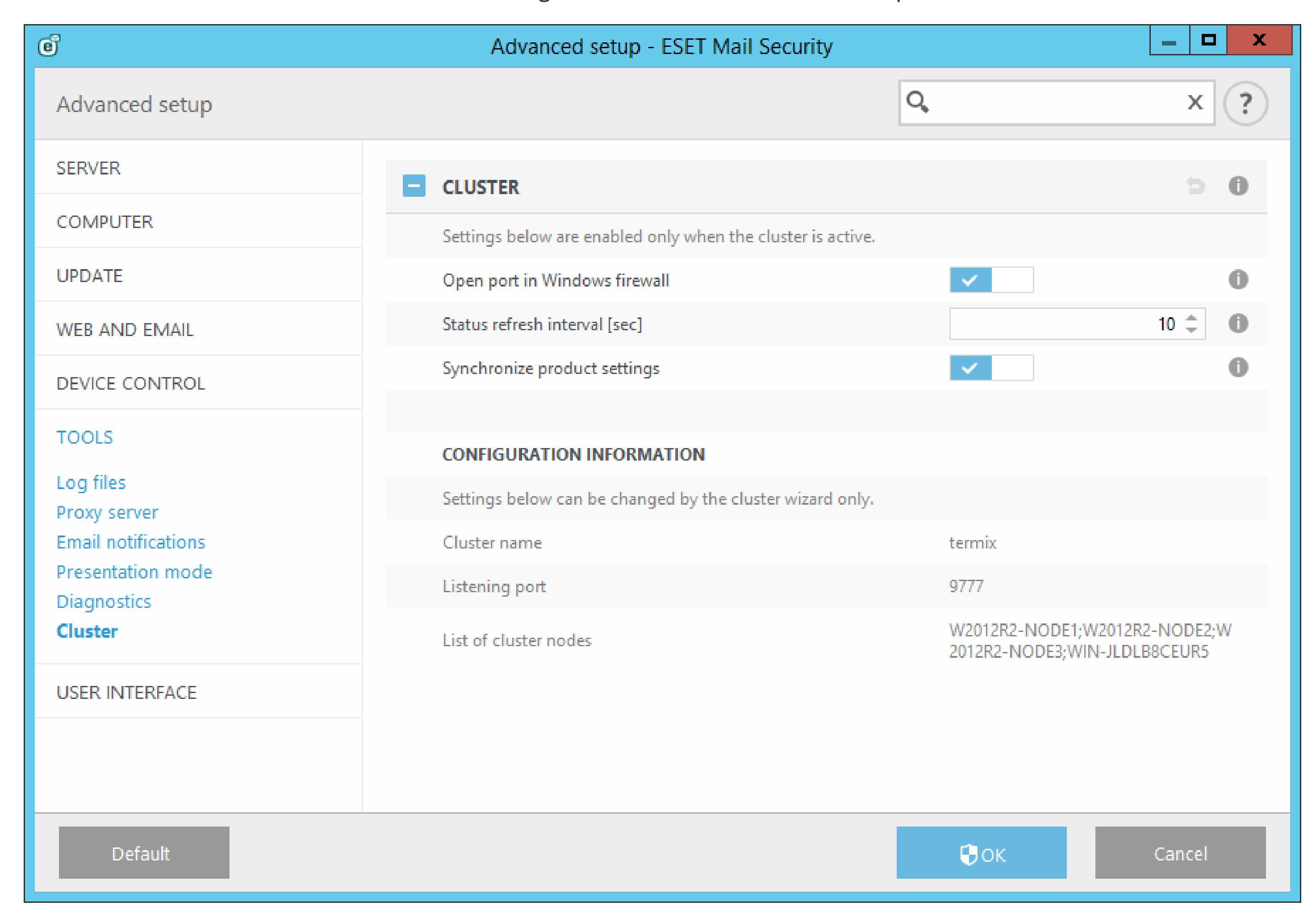
5.6.12 Cluster

L'option **Activer le cluster** est activée automatiquement lorsqu'ESET Cluster est configuré. Vous pouvez la désactiver manuellement dans la fenêtre Configuration avancée en cliquant sur l'icône de commutateur (cela est conseillé lorsque vous devez modifier la configuration sans affecter les autres nœuds d'ESET Cluster). Ce commutateur active ou désactive uniquement la fonctionnalité ESET Cluster. Pour configurer ou détruire correctement le cluster, il est nécessaire d'utiliser l'Assistant Cluster ou la commande Détruire le cluster située dans la section **Outils** > **Cluster** de la fenêtre principale du programme.

Fonctionnalité ESET Cluster non configurée et désactivée :



Fonctionnalité ESET Cluster correctement configurée avec ses informations et options :



Pour plus d'informations sur ESET Cluster, cliquez ici.

5.7 Interface utilisateur

La section **Interface utilisateur** permet de configurer le comportement de l'interface utilisateur graphique (GUI) du programme. Vous pouvez ajuster l'apparence du programme et l'utilisation des effets.

Pour bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute modification non autorisée à l'aide de l'outil Configuration de l'accès.

En configurant Alertes et notifications, vous pouvez modifier le comportement des alertes concernant les menaces détectées et les notifications système. Ces alertes peuvent être personnalisées en fonction de vos besoins.

Si vous choisissez de ne pas afficher certaines notifications, ces dernières apparaissent dans la zone États et messages désactivés. Vous pouvez vérifier leur état, afficher des détails supplémentaires ou supprimer des notifications de cette fenêtre.

L'intégration dans le menu contextuel s'affiche lorsque vous cliquez avec le bouton droit sur l'objet sélectionné. Utilisez cet outil pour intégrer les options ESET Mail Security au menu contextuel.

Le mode de présentation est utile pour les utilisateurs qui souhaitent travailler dans une application sans être interrompus par des fenêtres contextuelles, des tâches planifiées et tout autre composant qui pourrait réquisitionner les ressources système.

Éléments de l'interface utilisateur

La configuration de l'interface utilisateur ESET Mail Security peut être modifiée de manière à adapter l'environnement de travail à vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur** > **Éléments de l'interface utilisateur** de l'arborescence Configuration avancée ESET Mail Security.

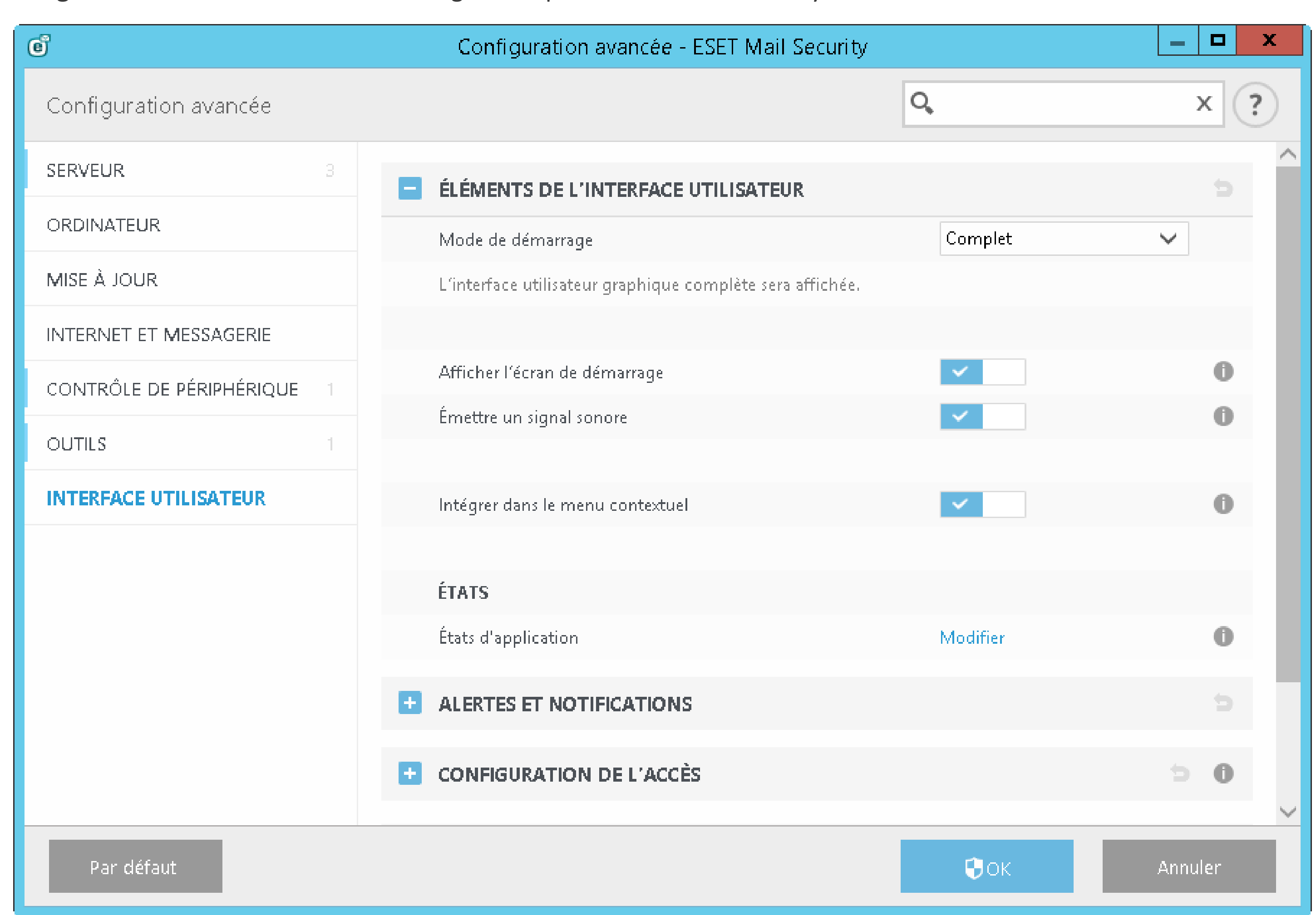
Dans la section **Éléments de l'interface utilisateur**, vous pouvez ajuster l'environnement de travail. L'interface utilisateur doit être définie sur le mode **Terminal** si les éléments graphiques ralentissent les performances de votre ordinateur ou entraînent d'autres problèmes. Vous souhaiterez peut-être également désactiver l'interface utilisateur graphique sur un serveur Terminal Server. Pour plus d'informations sur l'installation de ESET Mail Security sur un serveur Terminal Server, reportez-vous à la rubrique Désactiver l'interface utilisateur graphique sur un serveur Terminal Server.

Cliquez sur le menu déroulant **Mode de démarrage de l'interface utilisateur graphique** pour sélectionner un mode de démarrage de l'interface utilisateur graphique parmi les suivants :
Complet - L'intégralité de l'interface utilisateur graphique est affichée.
Terminal - Aucune notification ni alerte n'est affichée. L'interface utilisateur graphique peut être uniquement démarré par l'administrateur.

Pour désactiver l'écran de démarrage ESET Mail Security, désactivez **Afficher l'écran de démarrage**.

Pour qu'ESET Mail Security émette un signal sonore en cas d'événement important lors d'une analyse, par exemple lorsqu'une menace est découverte ou lorsque l'analyse est terminée, sélectionnez **Utiliser un signal sonore**.

Intégrer dans le menu contextuel - Intègre les options ESET Mail Security dans le menu contextuel.



États - Cliquez sur **Modifier** pour gérer (activer ou désactiver) les états affichés dans le volet Supervision du menu principal.

États d'application - Permet d'activer ou de désactiver l'affichage de l'état dans le volet **État de la protection** du menu principal.

5.7.1 Alertes et notifications

La section **Alertes et notifications** sous **Interface utilisateur** vous permet de configurer la manière dont ESET Mail Security traite les alertes de menace et les notifications système (par ex. les messages indiquant une mise à jour réussie). Vous pouvez également configurer l'heure d'affichage et la transparence des notifications dans la barre d'état système (cela ne s'applique qu'aux systèmes prenant en charge ces notifications).

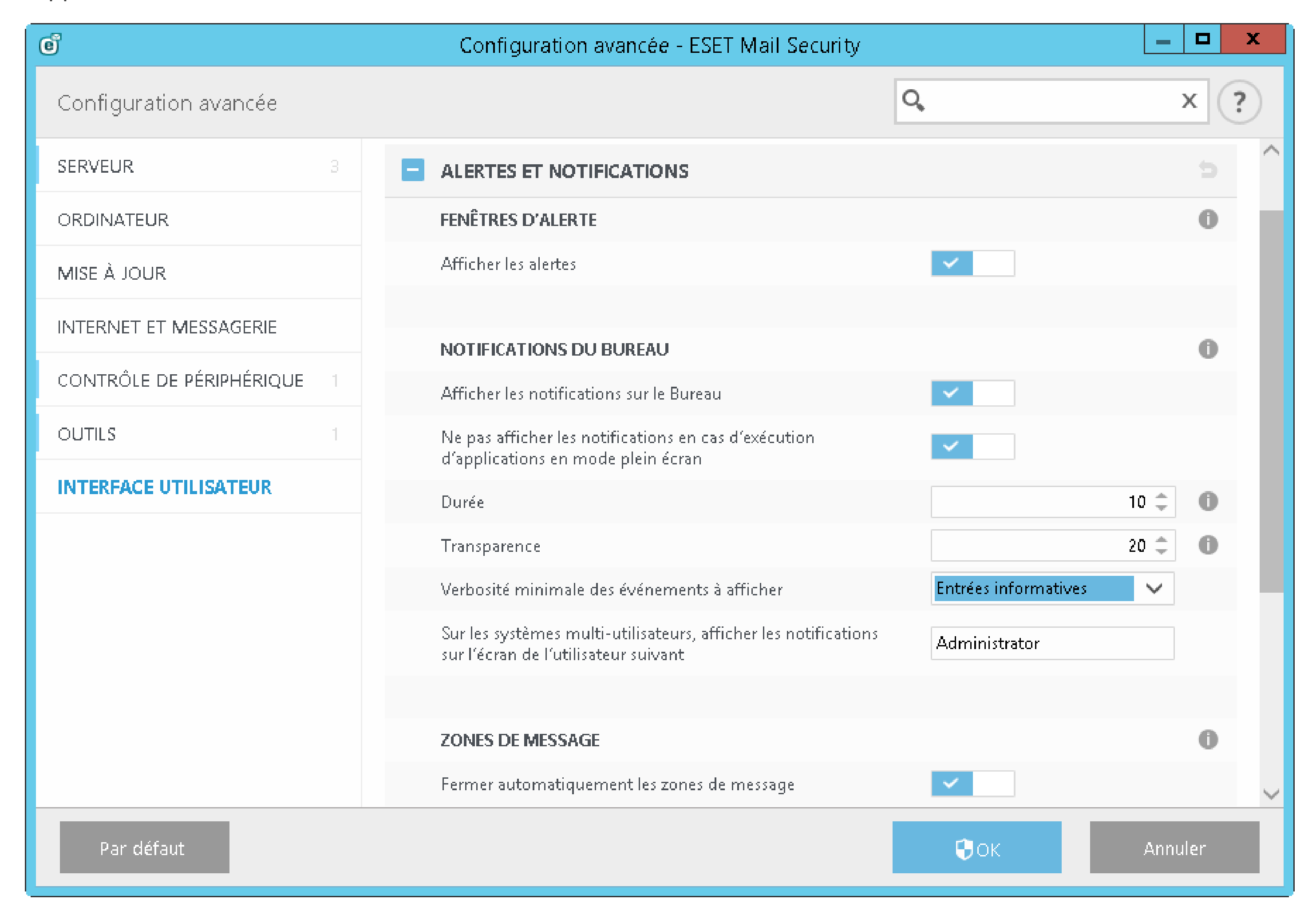
Fenêtres d'alerte

Lorsque l'option **Afficher les alertes** est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

Notifications du Bureau

Les notifications sur le Bureau et les info-bulles sont fournies à titre d'information uniquement et n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la partie système de la barre d'état, dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le Bureau, sélectionnez **Afficher les notifications sur le bureau**. D'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) peuvent être modifiées en dessous.

Activez l'option **Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives.



Zones de message

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez **Fermer automatiquement les zones de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Le menu déroulant **Verbosité minimale des événements à afficher** permet de sélectionner le niveau de gravité des

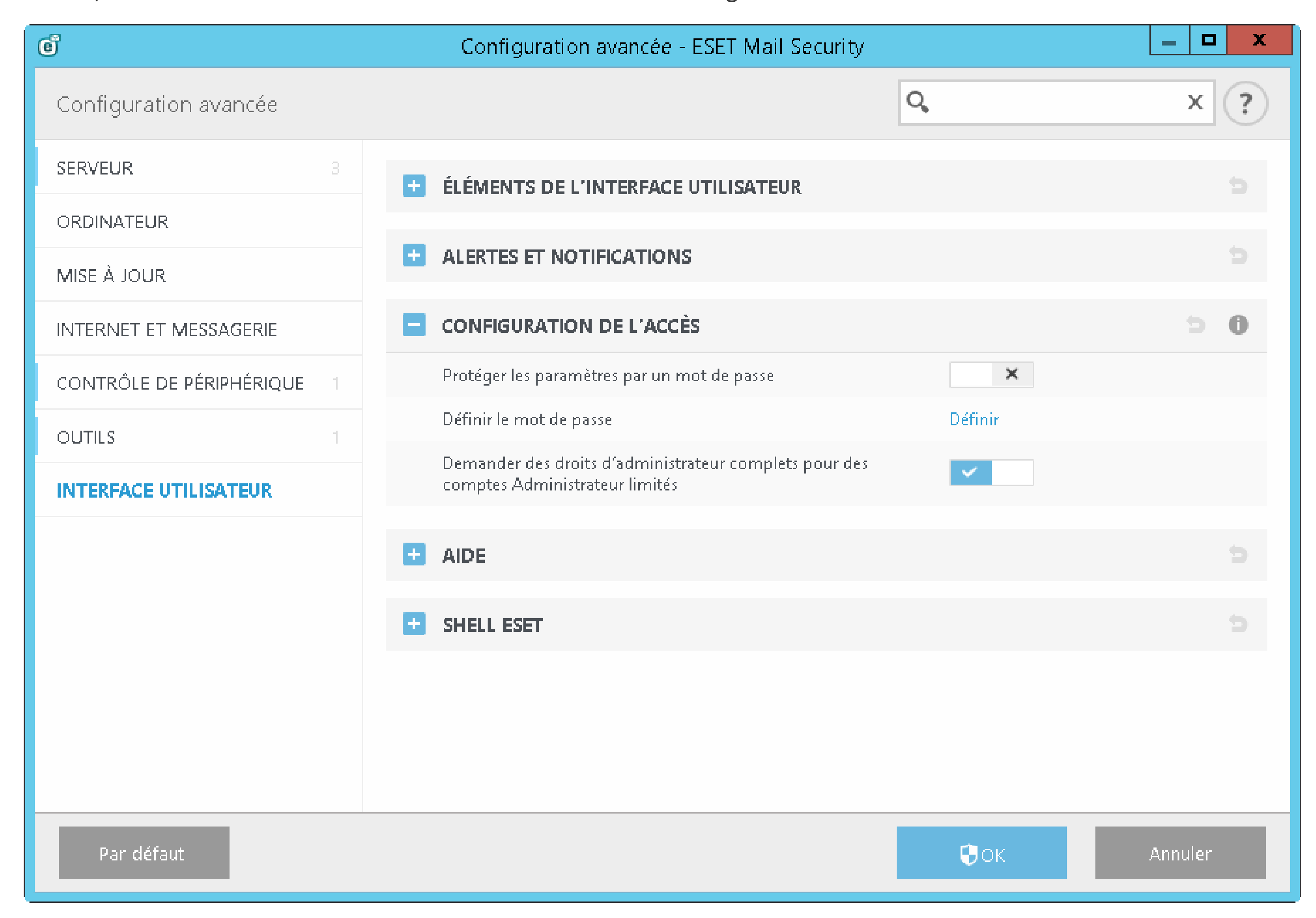
alertes et notifications à afficher. Les options disponibles sont les suivantes :

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** - Enregistre les erreurs du type « Erreur de téléchargement du fichier » et les erreurs critiques.
- **Critique** - Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus, etc.).

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. Le champ **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** indique l'utilisateur qui recevra les notifications système et les autres notifications lorsque le système autorise la connexion simultanée de plusieurs utilisateurs. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, à condition que toutes les notifications système soient envoyées à l'administrateur.

5.7.2 Configuration de l'accès

Il est essentiel que ESET Mail Security soit correctement configuré pour garantir la sécurité maximale du système. Tout changement inapproprié peut entraîner la perte de données importantes. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Mail Security peuvent être protégés par mot de passe. Les paramètres de configuration pour la protection par mot de passe figurent dans le sous-menu **Configuration de l'accès**, sous **Interface utilisateur** dans l'arborescence de la configuration avancée.



Protection des paramètres par mot de passe - Verrouille ou déverrouille les paramètres de configuration du programme. Cliquez sur cette option pour ouvrir la fenêtre Configuration du mot de passe.

Pour définir ou modifier un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir le mot de passe**.

Demander des droits d'administrateur complets pour des comptes Administrateur limités - Sélectionnez cette option pour inviter l'utilisateur actuel (s'il ne possède pas les autorisations d'administrateur) à saisir un nom d'utilisateur et un mot de passe d'administrateur lors de la modification de certains paramètres du système (semblable au contrôle UAC dans Windows Vista). Elles portent également sur la désactivation des modules de protection.

5.7.2.1 Mot de passe

Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Mail Security peuvent être protégés par mot de passe.

5.7.2.2 Configuration du mot de passe

Pour protéger les paramètres de configuration d'ESET Mail Security afin d'éviter toute modification non autorisée, vous devez définir un nouveau mot de passe. Si vous souhaitez modifier un mot de passe existant, tapez votre ancien mot de passe dans le champ **Ancien mot de passe**, saisissez votre nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **OK**. Vous aurez besoin de ce mot de passe pour les prochaines modifications d'ESET Mail Security.

5.7.3 Aide

Lorsque vous appuyez sur la touche **F1** ou que vous cliquez sur le bouton **?**, une fenêtre d'aide en ligne s'ouvre. C'est la principale source de contenu d'aide. Il existe également une copie hors ligne de l'aide qui est installée avec le programme. L'aide hors ligne s'ouvre en cas d'absence de connexion Internet.

La dernière version de l'aide en ligne s'affiche automatiquement lorsque vous disposez d'une connexion Internet.

5.7.4 Shell ESET

Vous pouvez configurer les droits d'accès aux données, fonctionnalités et paramètres du produit par l'intermédiaire d'eShell en changeant la **Politique d'exécution du Shell ESET**. Le paramètre par défaut est **Scripts limités**, mais vous pouvez le modifier et choisir **Désactivé**, **Lecture seule** ou **Accès complet**, si nécessaire.

- **Désactivé** : eShell ne peut pas être utilisé. Seule la configuration d'eShell est autorisée dans le contexte `ui eshell`. Vous pouvez personnaliser l'aspect d'eShell, mais vous ne pouvez pas accéder aux paramètres ou données du produit.
- **Lecture seule** : eShell peut être utilisé comme outil de surveillance. Vous pouvez afficher tous les paramètres dans les modes de traitement par lots et interactif. Vous ne pouvez toutefois pas modifier les paramètres, les fonctionnalités ni les données.
- **Scripts limités** : en mode interactif, vous pouvez afficher l'ensemble des paramètres, des fonctionnalités et des données. En mode de traitement par lots, eShell fonctionne comme si vous étiez en mode de lecture seule. Toutefois, si vous utilisez des fichiers de commandes signés, vous ne pouvez pas modifier les paramètres ni les données.
- **Accès complet** : l'accès à tous les paramètres est illimité dans les modes interactif et de traitement par lots. Vous pouvez afficher et modifier les paramètres. Pour exécuter eShell avec un accès complet, vous devez utiliser un compte d'administrateur. Si la fonctionnalité Contrôle de compte d’utilisateur (UAC) est activée, une élévation est également requise.

5.7.5 Désactivation de l'interface utilisateur graphique sur Terminal Server

Ce chapitre indique comment désactiver l'interface utilisateur graphique d'ESET Mail Security sur Windows Terminal Server pour les sessions utilisateur.

Normalement, l'interface utilisateur graphique d'ESET Mail Security démarre chaque fois qu'un utilisateur distant se connecte au serveur et crée une session de terminal. Cet affichage n'est généralement pas conseillé sur les serveurs Terminal Server. Si vous souhaitez désactiver l'interface utilisateur graphique pour les sessions de terminal, vous pouvez le faire par le biais d'eShell en exécutant la commande `set ui ui gui-start-mode terminal`. L'interface utilisateur graphique passe ainsi en mode terminal. Il existe deux modes pour le démarrage de l'interface utilisateur graphique :

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

Si vous souhaitez connaître le mode actuellement utilisé, exécutez la commande `get ui ui gui-start-mode`.

REMARQUE : si vous avez installé ESET Mail Security sur un serveur Citrix, il est recommandé d'utiliser les paramètres décrits dans cet article de la base de connaissances.

5.7.6 États et messages désactivés

Messages de confirmation - Affiche la liste des messages de confirmation que vous pouvez choisir d'afficher ou non.

États d'application désactivés - Permet d'activer ou de désactiver l'affichage de l'état dans le volet **État de la protection** du menu principal.

5.7.6.1 Messages de confirmation

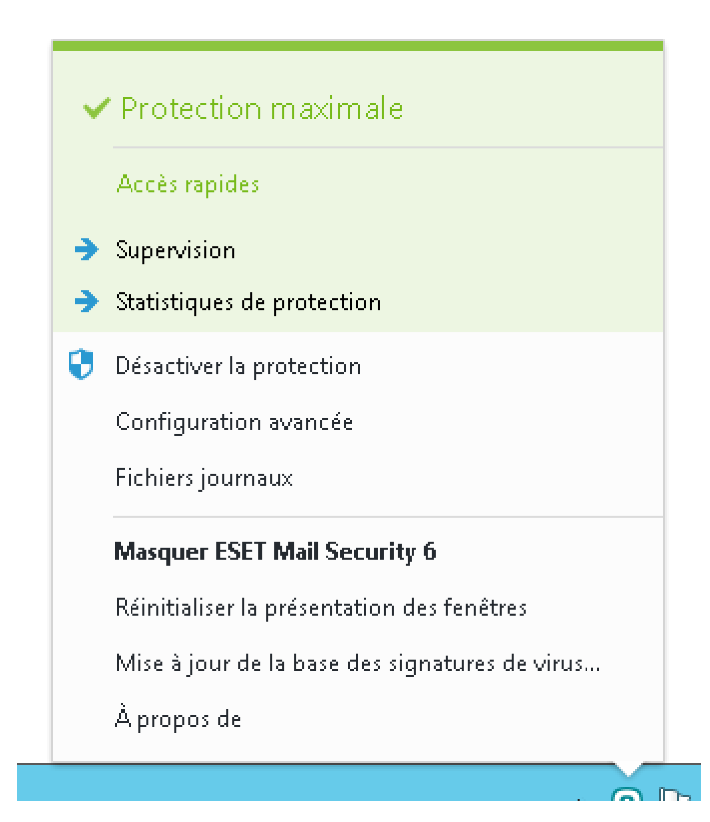
Cette boîte de dialogue contient les messages de confirmation qu'ESET Mail Security affiche avant l'exécution de toute action. Activez ou désactivez la case à cocher en regard de chaque message de confirmation pour l'activer ou non.

5.7.6.2 États d’application désactivés

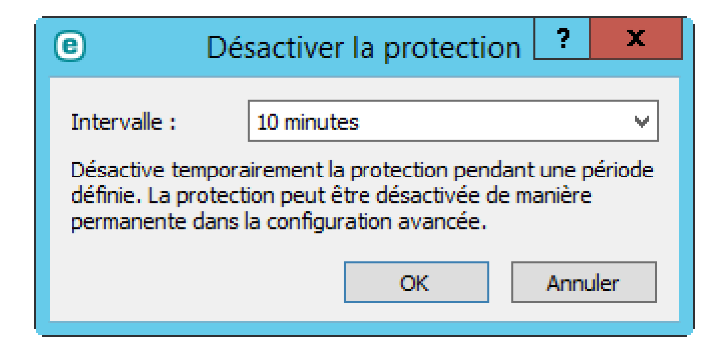
Cette boîte de dialogue permet de sélectionner les états d'application à afficher ou non, par exemple lorsque vous interrompez la protection antivirus et antispyware ou lorsque vous activez le mode de présentation. Un état d'application est également affiché si votre produit n'est pas activé ou si la licence est arrivée à expiration.

5.7.7 Icône dans la partie système de la barre des tâches

Pour accéder à certaines des fonctionnalités et options de configuration les plus importantes, cliquez avec le bouton droit sur l'icône dans la partie système de la barre des tâches.



Désactiver la protection - Affiche la boîte de dialogue de confirmation qui désactive la protection antivirus et antispyware ; cette dernière protège des attaques malveillantes en contrôlant les fichiers et les communications par messagerie et Internet.



Le menu déroulant **Intervalle** indique la durée pendant laquelle la protection antivirus et antispyware est désactivée.

Configuration avancée - Sélectionnez cette option pour afficher l'arborescence **Configuration avancée**. Vous pouvez également accéder à Configuration avancée en appuyant sur la touche F5 ou en accédant à **Configuration** > **Configuration avancée**.

Fichiers journaux - Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées.

MasquerESET Mail Security - Masque la fenêtre ESET Mail Security.

Réinitialiser la disposition des fenêtres - Rétablit la taille et la position par défaut de la fenêtre ESET Mail Security.

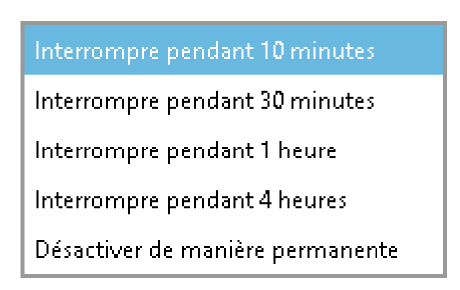
Mise à jour de la base des signatures de virus - Commence la mise à jour de la base des signatures des virus afin de garantir un niveau optimal de protection contre les codes malveillants.

À propos - Les informations système fournissent des détails sur la version installée d'ESET Mail Security, sur les modules installés et sur la date d'expiration de votre licence. Des informations sur votre système d'exploitation et

les ressources système figurent dans la partie inférieure de la page.

5.7.7.1 Désactiver la protection

Chaque fois que vous désactivez temporairement les modules antivirus ou antispyware à l'aide de l'icône dans la partie système de la barre des tâches, la boîte de dialogue **Désactiver temporairement la protection** s'affiche. La protection contre les logiciels malveillants est alors désactivée pendant la période sélectionnée (pour désactiver la protection de manière permanente, vous devez utiliser l'option Configuration avancée). Soyez prudent. La désactivation de la protection peut exposer votre système à des menaces.

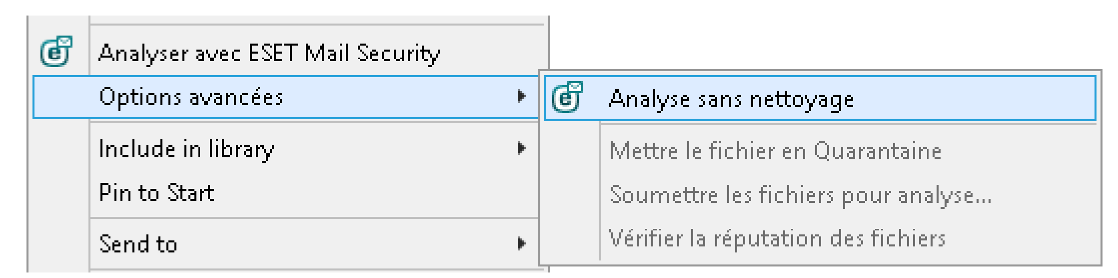


5.7.8 Menu contextuel

Le menu contextuel est le menu qui s'affiche lorsque vous cliquez avec le bouton sur un objet (fichier). Il répertorie toutes les actions que vous pouvez effectuer sur un objet.

Il est possible d'intégrer les options ESET Mail Security dans le menu contextuel. Les options de configuration de cette fonctionnalité figurent dans l'arborescence de la configuration avancée, sous **Interface utilisateur** > **Éléments de l'interface utilisateur**.

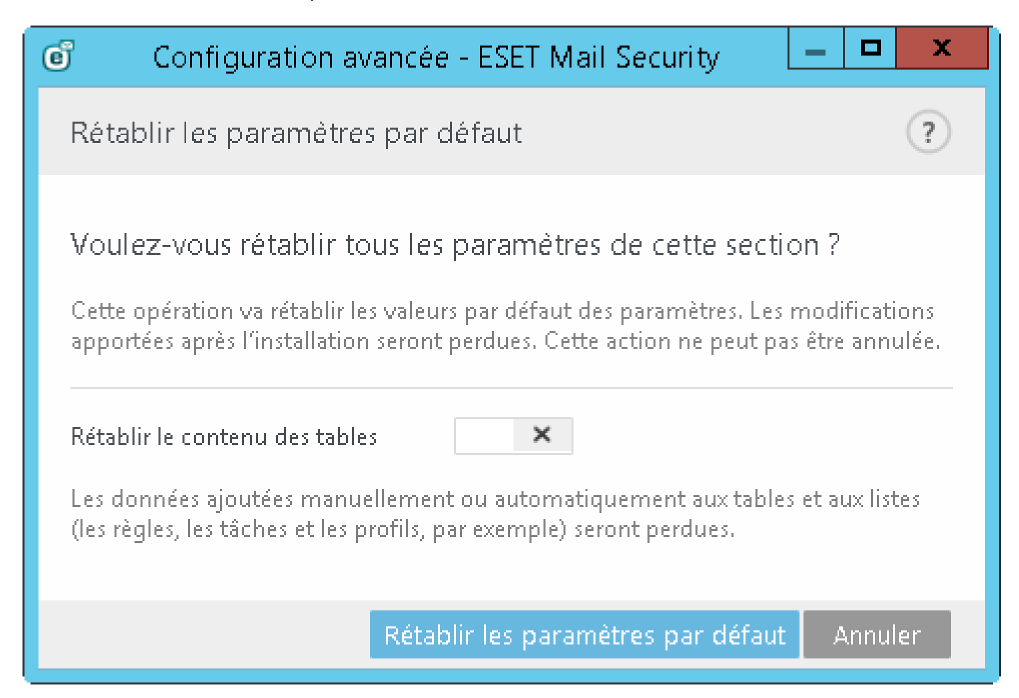
Intégrer dans le menu contextuel - Intègre les options ESET Mail Security dans le menu contextuel.



5.8 Rétablir tous les paramètres de cette section

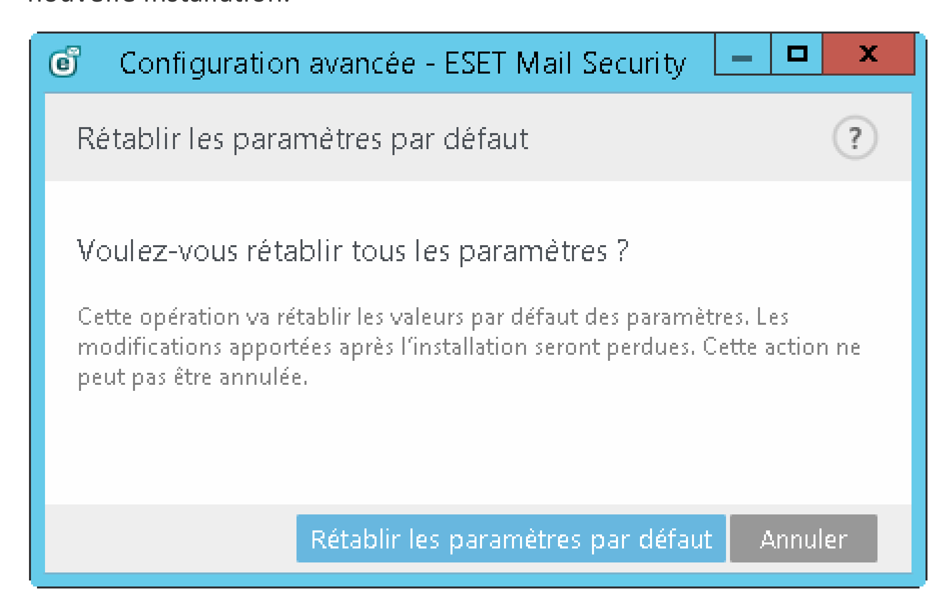
Rétablit les paramètres de module par défaut définis par ESET. Notez que les modifications apportées après avoir cliqué sur **Rétablir les paramètres par défaut** sont perdues.

Rétablir le contenu des tables : lorsque cette option est activée, les tâches ou les profils ajoutés automatiquement ou manuellement sont perdus.



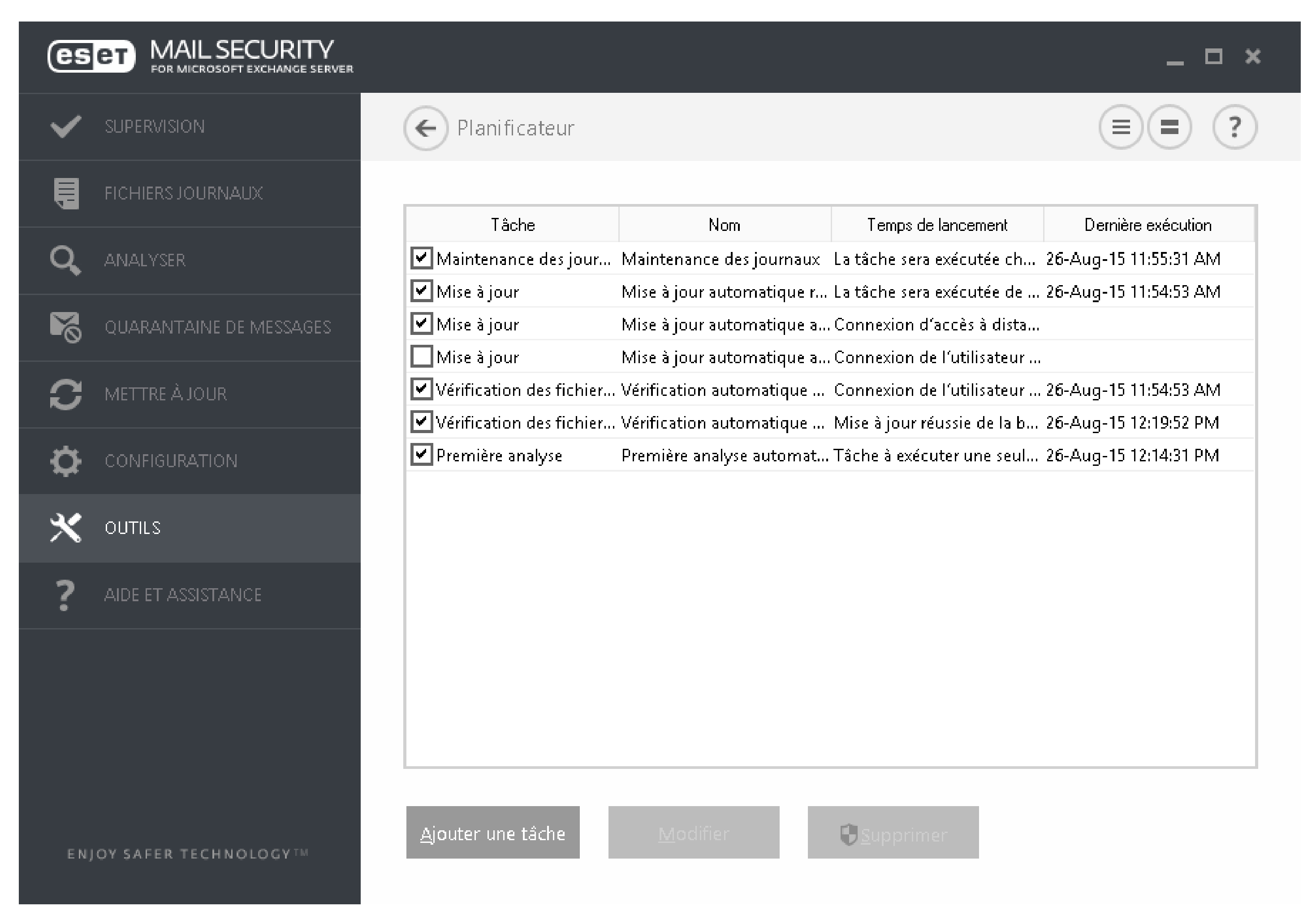
5.9 Rétablir les paramètres par défaut

Tous les paramètres du programme, pour tous les modules, sont rétablis dans l'état qu'ils auraient après une nouvelle installation.



5.10 Planificateur

Le **Planificateur** est accessible depuis le menu principal d'ESET Mail Security, dans **Outils**. Le planificateur contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes sont affichées dans le **Planificateur** :

- **Maintenance des journaux**
- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification automatique des fichiers de démarrage**
- **Vérification automatique des fichiers de démarrage après la mise à jour réussie de la base des signatures de virus**
- **Première analyse automatique**

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier...** Vous pouvez également sélectionner la tâche à modifier et cliquer sur le bouton **Modifier...**

5.10.1 Détails de la tâche

Saisissez le nom de la tâche, sélectionnez un **type de tâche**, puis cliquez sur **Suivant** :

- **Exécuter une application externe**
- **Maintenance des journaux**
- **Contrôle des fichiers de démarrage du système**
- **Créer un rapport de l'état de l'ordinateur**
- **Analyse de l'ordinateur à la demande**
- **Première analyse**
- **Mise à jour**

Exécution de tâche : la tâche spécifiée est exécutée une fois, à la date et à l'heure indiquées.

Une tâche peut être ignorée si l'ordinateur est éteint ou alimenté par batterie. Sélectionnez à quel moment la tâche doit être exécutée parmi ces options, puis cliquez sur **Suivant** :

- À la prochaine heure planifiée
- Dès que possible
- Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée (heures)

5.10.2 Planification de la tâche - Une fois

Exécution de tâche : la tâche spécifiée est exécutée une fois, à la date et à l'heure indiquées.

5.10.3 Planification de la tâche

La tâche est exécutée de manière répétée aux intervalles indiqués. Sélectionnez l'une des options de planification suivantes :

- **Une fois** - La tâche est exécutée une fois, à la date et à l'heure prédéfinies.
- **Plusieurs fois** - La tâche est exécutée aux intervalles indiqués (en heures).
- **Quotidiennement** - La tâche est exécutée tous les jours à l'heure définie.
- **Chaque semaine** - La tâche est exécutée une ou plusieurs fois par semaine, au(x) jour(s) et à l'heure indiqués.
- **Déclenchée par un événement** - La tâche est exécutée après un événement particulier.

Ignorer la tâche en cas d'alimentation par batterie - Une tâche ne démarre pas si l'ordinateur est alimenté par batterie au moment de l'exécution prévue. Ceci s'applique également aux ordinateurs alimentés par un onduleur.

5.10.4 Planification de la tâche - Quotidiennement

La tâche va s'exécuter tous les jours à l'heure définie.

5.10.5 Planification de la tâche - Hebdomadairement

La tâche est exécutée le jour et l'heure définis.

5.10.6 Planification de la tâche - Déclenchée par un événement

La tâche peut être déclenchée par l'un des événements suivants :

- **Chaque fois que l'ordinateur démarre**
- **Au premier démarrage de l'ordinateur chaque jour**
- **Connexion d'accès à distance à Internet/au réseau VPN**
- **Mise à jour réussie de la base des signatures de virus**
- **Mise à jour réussie des composants du programme**
- **Ouverture de session utilisateur**
- **Détection de menace**

Lors de la planification d'une tâche déclenchée par un événement, vous pouvez indiquer l'intervalle minimum entre deux exécutions de la tâche. Par exemple, si vous ouvrez une session sur l'ordinateur plusieurs fois par jour,

choisissez un intervalle de 24 heures afin de réaliser la tâche uniquement à la première ouverture de session de la journée, puis le lendemain.

5.10.7 Détails de la tâche - Exécuter l'application

Cet onglet permet de programmer l'exécution d'une application externe.

- **Fichier exécutable** - Choisissez un fichier exécutable dans l'arborescence, cliquez sur l'option **...** ou saisissez le chemin manuellement.
- **Dossier de travail** - Définissez le répertoire de travail de l'application externe. Tous les fichiers temporaires du **fichier exécutable** sélectionné sont créés dans ce répertoire.
- **Paramètres** - Paramètres de ligne de commande de l'application (facultatif).

Cliquez sur **Terminer** pour appliquer la tâche.

5.10.8 Tâche ignorée

Si la tâche n'a pas pu être exécutée au moment défini, vous pouvez désigner le moment auquel elle doit être exécutée :

- **À la prochaine heure planifiée** - La tâche est exécutée à l'heure indiquée (après 24 heures, par exemple).
- **Dès que possible** - La tâche s'exécute dès que possible, c'est-à-dire dès que les actions qui empêchent son exécution ne sont plus valides.
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** - **Durée écoulée depuis la dernière exécution (heures)** - Lorsque vous sélectionnez cette option, votre tâche est toujours répétée après le nombre d'heures indiqué.

5.10.9 Détails des tâches du planificateur

Cette boîte de dialogue affiche des informations détaillées sur la tâche planifiée sélectionnée lorsque vous double-cliquez sur une tâche personnalisée ou que vous cliquez avec le bouton droit sur une tâche personnalisée du planificateur et cliquez sur **Afficher les détails des tâches**.

5.10.10 Profils de mise à jour

Pour mettre à jour le programme à partir de deux serveurs de mise à jour, vous devez créer deux profils de mise à jour distincts. Si le premier ne permet pas de télécharger les fichiers de mise à jour, le programme bascule automatiquement vers le second. Ce procédé est notamment adapté aux portables dont la mise à jour s'effectue normalement depuis un serveur de mise à jour du réseau local, mais dont les propriétaires se connectent souvent à Internet à partir d'autres réseaux. Par conséquent, en cas d'échec du premier profil, le second télécharge automatiquement les fichiers de mise à jour à partir des serveurs de mise à jour d'ESET.

Pour plus d'informations sur les profils de mise à jour, consultez la rubrique Mise à jour.

5.10.11 Création de nouvelles tâches

Pour créer une tâche dans le planificateur, cliquez sur le bouton **Ajouter une tâche** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe** - Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** - Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Créer un rapport de l'état de l'ordinateur** : crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** : effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Première analyse** : par défaut, 20 minutes après une installation ou un redémarrage, une analyse de l'ordinateur sera effectuée en tant que tâche de faible priorité.
- **Mise à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules de l'application.

La tâche planifiée la plus fréquente étant la **mise à jour**, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Saisissez un nom de tâche dans le champ **Nom de la tâche**. Dans le menu déroulant **Type de tâche**, sélectionnez **Mise à jour**, puis cliquez sur **Suivant**.
Activez le bouton bascule **Activé** si vous souhaitez activer la tâche (vous pouvez le faire ultérieurement en activant/ désactivant la case à cocher correspondante dans la liste des tâches planifiées). Cliquez ensuite sur **Suivant** et sélectionnez une des options de planification :
Une fois, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous serez invité à choisir différents paramètres de mise à jour. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée** (l'intervalle peut être spécifié dans la zone de liste déroulante Durée écoulée depuis la dernière exécution)

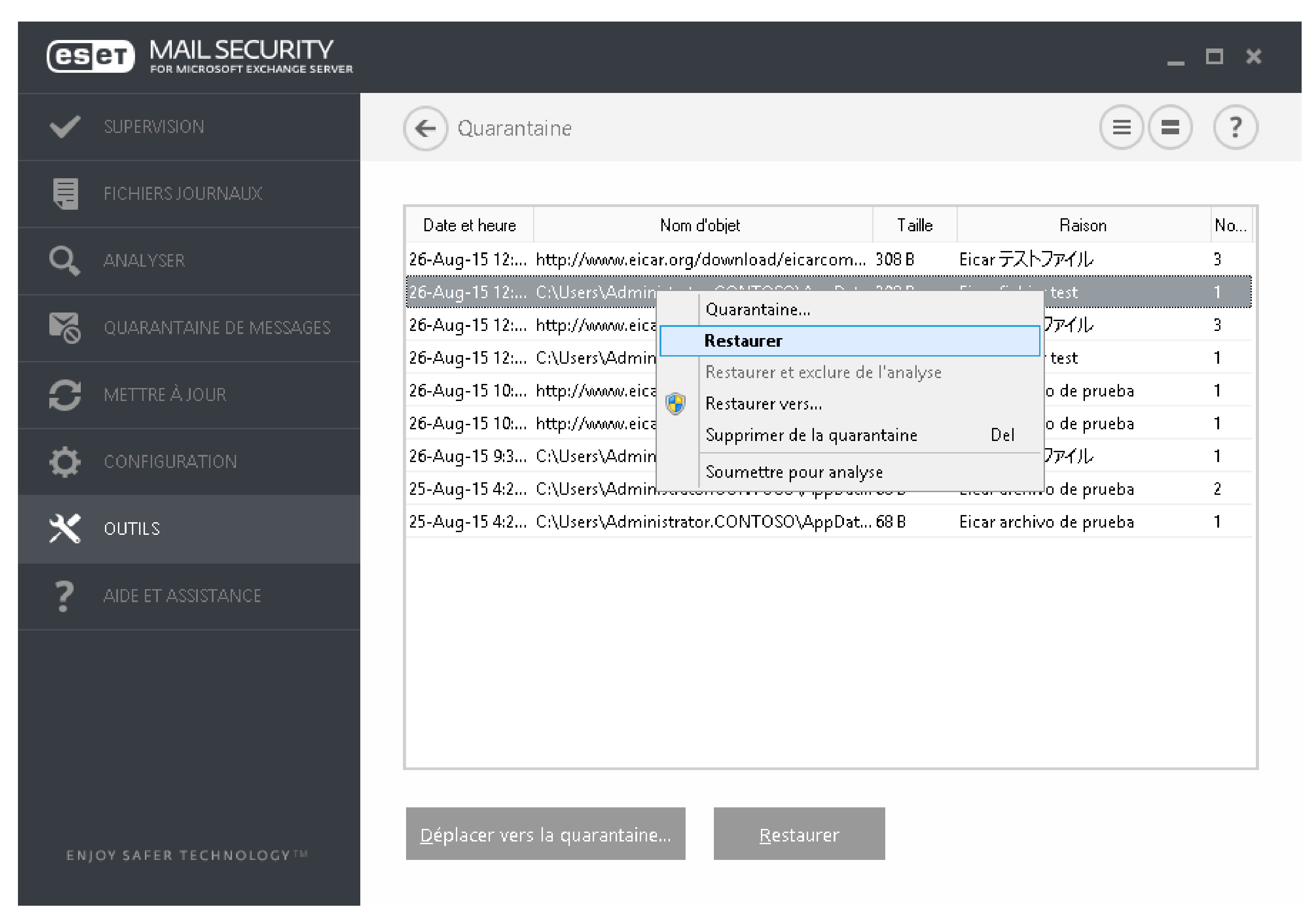
À l'étape suivante, une fenêtre de synthèse apparaît. Elle contient des informations sur la tâche planifiée actuelle. Lorsque vous avez terminé vos modifications, cliquez sur **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. Vous pouvez y définir le profil principal et le profil secondaire. Le profil secondaire est utilisé si la tâche ne peut pas être terminée à l'aide du profil principal. Cliquez sur **Terminer** pour ajouter la nouvelle tâche planifiée à la liste des tâches planifiées.

5.11 Quarantaine

La principale fonction de la quarantaine est de stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Mail Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte, mais n'a pas été détecté par l'analyseur antivirus. Les fichiers en quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple, objet ajouté par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple).

Mise en quarantaine de fichiers

ESET Mail Security met automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désactivé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine.** Les fichiers d'origine sont supprimés de leur emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Quarantaine**.

Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. L'option **Restaurer** est disponible dans le menu contextuel accessible en cliquant avec le bouton droit sur le fichier dans le fenêtre Quarantaine. Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est également disponible. Pour en savoir plus sur ce type d'application, consultez le glossaire. Le menu contextuel propose également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

i **REMARQUE :** si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service client d'ESET.

Soumission de fichiers mis en quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

5.11.1 Mise en quarantaine de fichiers

ESET Mail Security met automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désactivé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine**. Dans ce cas, le fichier d'origine n'est pas supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Quarantaine**.

5.11.2 Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour restaurer un fichier en quarantaine, cliquez avec le bouton droit dessus dans la fenêtre Quarantaine, puis sélectionnez **Restaurer** dans le menu contextuel. Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est également disponible. Le menu contextuel contient également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

Suppression d'un élément en quarantaine : cliquez avec le bouton droit sur un élément donné, puis sélectionnez **Supprimer l'élément en quarantaine**. Vous pouvez également sélectionner l'élément à supprimer, puis appuyer sur **Suppr** sur votre clavier. Vous pouvez aussi sélectionner plusieurs éléments et les supprimer simultanément.

i **REMARQUE**: si le programme met en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service client ESET.

5.11.3 Soumission de fichiers de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier de la quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre pour analyse** dans le menu contextuel.

5.12 Mises à jour du système d'exploitation

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles prêtes pour le téléchargement et l'installation. Le niveau de priorité de chaque mise à jour s'affiche à côté de son nom.

Cliquez sur **Exécuter une mise à jour système** pour lancer le téléchargement et l'installation des mises à jour du système d'exploitation.

Cliquez avec le bouton droit sur une ligne de mise à jour et cliquez sur **Afficher les informations** pour afficher une fenêtre contextuelle comportant des informations supplémentaires.

6. Glossaire

6.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

6.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même (accidentellement ou délibérément) le programme malveillant.

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux logiciels espions, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

Dans la catégorie des virus, on peut citer : OneHalf, Tenga et Yankee Doodle.

6.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

Parmi les vers les plus connus, on peut citer : Lovsan/Blaster, Stration/Warezov, Bagle et Netsky.

6.1.3 Chevaux de Troie

Dans le passé, les chevaux de Troie étaient définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Il est cependant important de remarquer que cette définition s'applique aux anciens chevaux de Troie. Aujourd'hui, il ne leur est plus utile de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Downloader (Téléchargeur)** : programme malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- **Dropper (Injecteur)** : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor (Porte dérobée)** : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- **Keylogger** (enregistreur de frappe) : programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- **Composeur** : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque la création d'une nouvelle connexion. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Les chevaux de Troie prennent généralement la forme de fichiers exécutables avec l'extension .exe. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer : NetBus, Trojandownloader. Small.ZL, Slapper

6.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Il existe deux niveaux de détection permettant d'éviter les rootkits :

1) Lorsqu'ils essaient d'accéder au système. Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).
2) Lorsqu'ils sont inaccessibles aux tests habituels. Les utilisateurs ESET Mail Security bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

6.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires en tant que tels ne sont pas dangereux ; ils dérangent simplement les utilisateurs en affichant des publicités. Le danger réside dans le fait qu'ils peuvent également avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un programme publicitaire. Dans la plupart des cas, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, deux précautions valent mieux qu'une. Si un fichier est détecté comme logiciel publicitaire sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

6.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme logiciel espion sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

6.1.7 Compresseurs

Le compresseur est un fichier exécutable auto-extractible qui associe plusieurs genres de programmes malveillants dans un seul package.

Les compresseurs les plus courants sont UPX, PE_Compact, PKLite et ASPack. Le même programme malveillant peut être détecté différemment lorsqu'il est compressé à l'aide d'un compresseur différent. Les compresseurs sont capables de faire muter leur « signature » au fil du temps, les programmes malveillants deviennent ainsi plus difficiles à détecter et à supprimer.

6.1.8 Bloqueur d'exploit

Le bloqueur d'exploit est conçu pour renforcer les applications connues pour être très vulnérables aux exploits (navigateurs Web, lecteurs de fichiers PDF, clients de messagerie et composants MS Office). Il surveille le comportement des processus et recherche toute activité suspecte pouvant indiquer un exploit. Il offre une couche de protection supplémentaire, plus proche des pirates, en utilisant une technologie complètement différente par rapport aux techniques axées uniquement sur la détection des fichiers malveillants.

Lorsqu'il identifie un processus suspect, le bloqueur d'exploit peut arrêter ce processus immédiatement. Il enregistre les données concernant la menace et les envoie au système ESET Live Grid dans le cloud. Ces données sont traitées par le laboratoire d'ESET et permettent de mieux protéger tous les utilisateurs contre les menaces inconnues et les attaques immédiates (logiciels malveillants très récents n'ayant encore aucun remède préconfiguré).

6.1.9 Scanner de mémoire avancé

Le scanner de mémoire avancé fonctionne avec le bloqueur d'exploit pour offrir une meilleure protection contre les logiciels malveillants qui ne sont pas détectés par les produits anti-logiciels malveillants grâce à l'obscurcissement et/ou au chiffrement. Dans les cas où l'émulation ou l'heuristique classique ne détecte pas la menace, le scanner de mémoire avancé est en mesure d'identifier tout comportement suspect et d'analyser les menaces lorsqu'elles apparaissent dans la mémoire système. Cette solution est efficace même sur les logiciels malveillants fortement obscurcis. Contrairement au bloqueur d'exploit, il s'agit d'une méthode ultérieure à l'exécution. Cela signifie que des activités malveillantes ont pu avoir le temps de s'exécuter avant que cette menace soit détectée. Toutefois, si les autres techniques de détection ont échoué, il apporte une couche supplémentaire de sécurité.

6.1.10 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET Mail Security permet de détecter ces menaces.

La classification **Applications potentiellement dangereuses** s'utilise pour des logiciels authentiques du commerce. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous ne l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

6.1.11 Applications potentiellement indésirables

Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres (contextuelles, publicitaires) ;
- activation et exécution de processus cachés ;
- augmentation de l'utilisation des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

6.2 Courrier électronique

Le courrier électronique est une forme de communication moderne qui offre beaucoup d'avantages. Adaptable, rapide et direct, il a joué un rôle crucial dans l'expansion d'Internet au début des années 90.

Malheureusement, le grand anonymat des courriers électroniques et Internet a laissé libre champ aux activités illégales telles que le « spamming » (le fait d'envoyer des messages indésirables à un grand nombre de personnes). Les courriers indésirables comprennent les publicités indésirables, les canulars et les logiciels malveillants. Les désagréments et le danger augmentent, car l'envoi de tels messages ne coûte rien et les auteurs de courrier indésirable disposent de nombreux outils qui leur permettent de se procurer facilement de nouvelles adresses de messagerie. Par ailleurs, le volume et la variété du courrier indésirable ne facilitent pas la réglementation. Plus vous utilisez votre adresse de messagerie, plus vous augmentez la possibilité de tomber dans un moteur de base de données de courrier indésirable. Voici quelques conseils de prévention :

- Évitez de publier votre adresse de messagerie sur Internet.
- Ne donnez votre adresse de messagerie qu'à des personnes fiables.
- Évitez d'utiliser des pseudonymes communs : un pseudonyme compliqué est moins susceptible d'être traqué.
- Ne répondez pas au courrier indésirable qui est arrivé dans votre boîte de réception.
- Faites attention lorsque vous remplissez des formulaires sur Internet : soyez particulièrement attentif aux options du type « Oui, je voudrais recevoir des informations concernant ... ».
- Utilisez des adresses de messagerie « spécialisées », par exemple une adresse pour votre travail, une autre pour communiquer avec vos amis, etc.
- Changez vos adresses de messagerie de temps en temps.
- Utilisez une solution antispam.

6.2.1 Publicités

La publicité via Internet est une des formes de publicité les plus en vogue. D'un point de vue marketing, la publicité présente plusieurs avantages : ses coûts sont minimes, elle est très directe et les messages sont transmis presque immédiatement. De nombreuses entreprises utilisent des outils de marketing par courrier électronique pour communiquer de manière efficace avec leurs clients et prospects.

Ce mode de publicité est légitime, car vous pourriez être intéressé par la réception d'informations commerciales sur certains produits. Toutefois, de nombreuses entreprises envoient des masses de messages commerciaux non sollicités. La publicité par e-mail dépasse alors les limites et devient du courrier indésirable, ou spam.

La quantité de messages publicitaires non sollicités est devenue un réel problème, car elle ne montre aucun signe de ralentissement. Les auteurs de messages non sollicités tentent souvent de déguiser le courrier indésirable sous des dehors de messages légitimes.

6.2.2 Canulars

Un canular (ou hoax) est message propagé sur Internet. Il est envoyé généralement avec le courrier et parfois par des outils de communication tels que ICQ et Skype. Le message est souvent une blague ou une légende urbaine.

Les canulars essaient de provoquer chez les destinataires de la peur, de l'incertitude et du doute, les amenant à croire qu'un « virus indétectable » supprime tous les fichiers et récupère les mots de passe, ou effectue une activité nuisible sur leur système.

Certains canulars demandent aux destinataires de transmettre des messages à leurs contacts, ce qui a pour conséquence de propager les canulars. Même les téléphones portables reçoivent des canulars et des demandes d'aide (des personnes proposant par exemple de vous envoyer de l'argent depuis l'étranger). Il est souvent impossible de déterminer l'intention du créateur.

Si un message vous demande de le faire suivre à toutes vos connaissances, il peut très bien s'agir d'un canular. Sur

Internet, de nombreux sites spécialisés peuvent vérifier la légitimité d'un courrier. Avant de retransmettre un message que vous soupçonnez d'être un canular, faites d'abord une recherche sur Internet à son sujet.

6.2.3 Hameçonnage

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Son but est d'accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc.

La technique consiste généralement à envoyer un message électronique en se faisant passer pour une personne ou une entreprise digne de confiance (institution financière, compagnie d'assurance par exemple). Le message peut sembler tout à fait authentique et contenir des graphiques et contenus qui proviennent véritablement de la source dont il se réclame. Vous êtes invité à entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe. Toutes ces données, si elles sont soumises, peuvent facilement être volées et utilisées à des fins illégales.

Les banques, compagnies d'assurance et autres sociétés légales ne demandent jamais de noms d'utilisateur et de mots de passe dans un message non sollicité.

6.2.4 Reconnaissance du courrier indésirable

Généralement, peu d'indicateurs contribuent à identifier le courrier indésirable (messages non sollicités) dans une boîte à lettres. Si un message remplit au moins l'un des critères suivants, il s'agit probablement de courrier indésirable.

- L'adresse de l'expéditeur ne figure pas dans la liste de vos contacts.
- Le contenu du message concerne une grosse somme d'argent qui vous est offerte, mais vous devez fournir d'abord une petite somme.
- Vous devez entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe.
- Le message est écrit dans une langue étrangère.
- Le message vous propose d'acheter un produit qui ne vous intéresse pas. Si vous décidez de l'acheter quand même, vérifiez que l'expéditeur du message est fiable (consultez le fabricant original du produit).
- Quelques mots sont mal écrits pour pouvoir passer à travers le filtre de courrier indésirable. Par exemple, « vaigra » au lieu de « viagra », etc.

6.2.4.1 Règles

Dans le contexte des solutions de protection antispam et des clients de messagerie, les règles sont des outils permettant de manipuler les fonctions de messagerie. Elles se composent de deux parties logiques :

1) la condition (par exemple, un message entrant provenant d'une certaine adresse)

2) l'action (par exemple, la suppression du message ou son déplacement vers un dossier spécifique)

Le nombre de règles et leurs combinaisons varient en fonction de la solution de protection antispam. Ces règles servent de protection antispam (messages non sollicités). Exemples caractéristiques :

- Condition : un message entrant contient des mots habituellement utilisés dans le courrier indésirable. 2. Action : supprimer le message
- Condition : un message entrant contient une pièce jointe comportant l'extension .exe 2. Action : supprimer la pièce jointe et livrer le message dans la boîte aux lettres
- Condition : un message entrant arrive de votre employeur 2. Action : déplacer le message dans le dossier Travail

Nous vous recommandons d'utiliser une combinaison de règles des programmes de programme antispam afin de faciliter l'administration et d'améliorer le filtrage du courrier indésirable.

6.2.4.2 Filtre bayésien

Le filtrage bayésien est une méthode très efficace de filtrage des messages, utilisée par la plupart des produits de protection antispam. Il permet d'identifier les messages non sollicités avec grande précision et peut s'adapter à chaque utilisateur.

Le principe est le suivant : la première phase est une phase d'apprentissage. L'utilisateur doit désigner un nombre suffisant de messages entrants comme étant des messages légitimes ou du courrier indésirable (normalement 200/200). Le filtre analyse les deux catégories et apprend par exemple que le courrier indésirable contient généralement des mots tels que « rolex » ou « viagra », tandis que les messages légitimes sont envoyés par des parents ou à partir d'adresses figurant dans la liste des contacts de l'utilisateur. Si le nombre de messages traités est suffisant, le filtre bayésien peut affecter un certain « indice de spam » à chaque message et déterminer s'il est ou non un courrier indésirable.

Le principal avantage du filtre bayésien est sa souplesse. Par exemple, si un utilisateur est biologiste, tous les messages entrants concernant la biologie ou des champs d'études apparentés recevront généralement un indice de probabilité moindre. Si un message envoyé par un membre de la liste des contacts de l'utilisateur comprend des mots qui le classeraient normalement dans la catégorie des messages non sollicités, il est marqué comme légitime dans la mesure où les expéditeurs d'une liste de contacts réduisent la probabilité qu'il s'agisse d'un courrier indésirable.

6.2.4.3 Liste blanche

En général, une liste blanche est une liste de personnes ou d'éléments qui ont été acceptés ou ont obtenu une autorisation d'accès. Le terme « liste blanche de messagerie » définit la liste de contacts dont l'utilisateur souhaite recevoir les messages. Ces listes blanches sont basées sur des mots-clés recherchés dans une adresse électronique, des noms de domaines ou des adresses IP.

Si une liste blanche fonctionne en « mode exclusif », les messages de toutes les autres adresses, domaines ou adresses IP sont écartés. Si elle fonctionne en mode non exclusif, ces messages ne sont pas supprimés, mais filtrés d'une autre façon.

Une liste blanche fonctionne sur le principe opposé de la liste noire. Les listes blanches sont relativement faciles à maintenir, plus que les listes noires. Pour un meilleur filtrage du courrier indésirable, nous vous recommandons d'utiliser des listes blanches et des listes noires.

6.2.4.4 Liste noire

En général, une liste noire répertorie les personnes ou les éléments non acceptés ou interdits. Dans le monde virtuel, c'est une technique qui permet d'accepter des messages de tous les utilisateurs qui ne figurent pas sur cette liste.

Il existe deux types de listes noires : les listes créées par les utilisateurs dans l'application de protection antispam et les listes professionnelles mises à jour régulièrement. Ces dernières sont créées par des institutions spécialisées et sont disponibles sur Internet.

Il est essentiel d'utiliser les listes noires pour bloquer le courrier indésirable, mais elles sont très difficiles à tenir à jour, car de nouveaux éléments à bloquer apparaissent jour après jour. Nous recommandons d'utiliser à la fois une liste blanche et une liste noire pour mieux filtrer le courrier indésirable.

6.2.4.5 Contrôle côté serveur

Le contrôle côté serveur est une technique permettant d'identifier le courrier indésirable de masse d'après le nombre de messages reçus et les réactions des utilisateurs. Chaque message laisse une empreinte numérique unique en fonction de son contenu. Le numéro d'identification unique ne donne aucune information sur le contenu du message. Deux messages identiques ont une empreinte identique, tandis que des messages différents ont une empreinte différente.

Si un message est marqué comme courrier indésirable, son empreinte est envoyée au serveur. Si le serveur reçoit plusieurs empreintes identiques (correspondant à un certain message de courrier indésirable), cette empreinte est stockée dans la base des empreintes de courrier indésirable. Lorsqu'il analyse des messages entrants, le programme envoie les empreintes de ces messages au serveur. Le serveur renvoie des informations indiquant les empreintes qui correspondent à des messages déjà identifiés comme courrier indésirable par d'autres utilisateurs.